acatech DISKUTIERT

> SICHERHEITSFORSCHUNG – CHANCEN UND PERSPEKTIVEN

PETRA WINZER/
ECKEHARD SCHNIEDER/
FRIEDRICH-WILHELM BACH (Hrsg.)




acatech DISKUTIERT

> SICHERHEITSFORSCHUNG – CHANCEN UND PERSPEKTIVEN

PETRA WINZER/
ECKEHARD SCHNIEDER/
FRIEDRICH-WILHELM BACH (Hrsg.)








> INHALT

> EINFÜHRUNG 7

> THEMATISCHE UND BEGRIFFLICHE STRUKTURIERUNG DER AKTUELLEN SICHERHEITSFORSCHUNG 11

1 Zukunftstechnologien in der Sicherheitsforschung
Klaus Thoma/Birgit Drees/Tobias Leismann 13

2 Sicherheit: Systemanalyse und –design
Jürgen Beyerer/Jürgen Geisler/Anna Dahlem/Petra Winzer 39

3 Präzisierung des normativen Sicherheitsbegriffs durch formalisierte Begriffsbildung
Eckehard Schnieder/Lars Schnieder 73





4 Thesen zum Problemfeld technische Sicherheit aus juristischer Sicht
Klaus Vieweg 117

5 Sicherheits- und Risikoterminologie im Spannungsfeld von Technik und Recht
Thomas Regenfus/Klaus Vieweg 131

> RISIKOFORSCHUNG UND SICHERHEITSKULTUREN 145

1 Interdisziplinäre Risiko- und Sicherheitsforschung
Annely Rothkegel/Gerhard Banse/Ortwin Renn 147

2 Sicherheit, Risiko und Vertrauen
Ortwin Renn 163

3 Techniksicherheit und Sicherheitskulturen
Gerhard Banse 185

4 Sicherheitsmodelle und Kommunikationsrisiko
Annely Rothkegel 207

5 Gesellschaftliche Voraussetzungen und Folgen der Technisierung von Sicherheit
Thomas Würtenberger/Steffen Tanneberger 221

> AUSBILDUNG FÜR MEHR SICHERHEITSKOMPETENZ 241

1 Kompetenzen für die Sicherheit
Norbert Pfeil/Wolfram Risch 243

2 Verzahnung von Aus- und Weiterbildung – die Lösung für sich ständig ändernde Anforderungen?
Wolfram Risch 251

3 Kernkompetenzen für die Sicherheit: Wissenschaftlich-technische Kompetenz braucht Lehre und Forschung - ein Beispiel
Norbert Pfeil 273

4 Einstellungen und Einschätzungen von zukünftigen Entscheidern zum Thema IT-Sicherheit, Ergebnisse und Schlussfolgerungen einer DsiN-Studie 2008
Gerhard Knorz 289

> ZUR UMSETZUNG VON SICHERHEIT IN DER PRAXIS 303

1 „Forschung für die Zivile Sicherheit“ – Das nationale Sicherheitsforschungsprogramm
Andreas Hoffknecht/Olav Teichert/Axel Zweck 305

2 Herausforderungen für die zivile Sicherheitswirtschaft und -wissenschaft in Deutschland
Stefan von Senger und Etterlin 321

> AUTORENVERZEICHNIS 335






> EINFÜHRUNG

PETRA WINZER/ECKEHARD SCHNIEDER/FRIEDRICH-WILHELM BACH

Sicherheit ist ein Grundbedürfnis der Menschen und somit der Gesellschaft. Wissenschaft und Technik dienen dazu, dieses Grundbedürfnis zu befriedigen. Der Begriff der Sicherheit wird jedoch sehr heterogen verwendet. Diese Heterogenität setzt sich in den Modellen und Lösungskonzepten zur Gewährleistung von Sicherheit fort und demzufolge ist das Themenfeld Sicherheit durch ein breites Spektrum von Gegenständen und Fragestellungen gekennzeichnet. Ziel des Themennetzwerks Sicherheit von acatech – Deutsche Akademie der Technikwissenschaften ist es, eine Brücke zwischen der Safety- und Security-Forschung zu schlagen. Dazu ist es zunächst erforderlich, die unterschiedlichen wissenschaftlichen Auffassungen sowie die vielfältigen Aktivitäten systematisch zu bündeln.

Vor dem Hintergrund der wachsenden gesellschaftlichen Bedeutung des Themas Sicherheit hat acatech ein Themennetzwerk zum Querschnittsthema Sicherheit ins Leben gerufen. Das Themennetzwerk wird übergreifende Fragen der zivilen Sicherheitsforschung stellen und Handlungsempfehlungen erarbeiten. Im Juni 2008 fand die Auftaktsitzung des acatech Themennetzwerks Sicherheit statt. Dem Themennetzwerk gehören ausgewiesene Vertreter aus den Bereichen Safety und Security an. Um der Vielfältigkeit des Themas Sicherheit gerecht zu werden, haben sich die Mitwirkenden des Themennetzwerks zu folgenden Unterarbeitsgruppen zusammengefunden:

- Arbeitsgruppe zum Thema „Sicherheitsbegriff/Taxonomie“ unter der Leitung von Prof. Dr.-Ing. Eckehard Schnieder (Braunschweig)
- Arbeitsgruppe zum Thema „neue Technologien“ unter der Leitung von Prof. Dr. Klaus Thoma (Freiburg)
- Arbeitsgruppe zum Thema „Systemtheorie/Systems Engineering“ unter der Leitung von Prof. Dr.-Ing. Jürgen Beyerer (Karlsruhe)
- Arbeitsgruppe zum Thema „Risikoforschung und Sicherheitskulturen“ unter der Leitung von Prof. Dr. Ortwin Renn (Stuttgart)
- Arbeitsgruppe zum Thema „Bildung und Kompetenz“ unter der Leitung von PD Dr. Wolfram Risch (Chemnitz)



Die Arbeitsgruppe zum Thema „Sicherheitsbegriff/Taxonomie", die von Prof. Dr.-Ing. Schnieder geleitet wird, verfolgt das Ziel, auf der Grundlage eines interdisziplinären methodischen Ansatzes ein konsistentes Begriffsgebäude für den Begriff „Sicherheit" zu entwerfen. Dies wollen Wissenschaftler und Wissenschaftlerinnen verschiedenster Fachdisziplinen durch die integrative Verknüpfung von zuvor terminologisch stringent formulierten und formalisierten Teilbegriffssystemen erreichen. Als Ergebnis wird ein Begriffsgebäude entstehen, welches die Brücke zwischen „Safety" und „Security" schaffen kann. Dies bildet die Basis für die Weiterarbeit im acatech Themennetzwerk Sicherheit.

Die Diskussion in den verschiedenen Workshops des Themennetzwerks zeigte, dass ein gemeinsames Denkmodell erforderlich ist, um transdisziplinär mit Ingenieuren, Geistes-, Sozial- und Naturwissenschaftlern neue Lösungsansätze gemeinsam zu entwickeln, die gleichzeitig sowohl Security- als auch Safetyaspekte berücksichtigen. Ob und wie dies gelingen kann, daran arbeitet die Arbeitsgruppe unter Leitung von Prof. Dr.-Ing. Beyerer. Ihr Ziel ist es, mittels des „Systems Engineering" neue Denk- und Vorgehensmodelle zu entwickeln, die von Wissenschaftlern verschiedenster Fachdisziplinen genutzt werden können, um technische und soziotechnische Systeme ganzheitlich sicherheitsgerecht zu gestalten.

Die Arbeitsgruppe zum Thema „neue Technologien" unter der Leitung von Prof. Dr. Thoma hat zum Ziel, die Anforderungen zu ermitteln, die zukünftige Technologien aus der Sicht der ganzheitlichen Sicherheit erfüllen müssen. Kann sie ihr Ziel umsetzen, dann könnten diese in Folgeschritten mit den neuen Systemmodellen umgesetzt werden.




Dabei sind aber zwingend gesellschaftliche Entwicklungen zu beachten. Welche das sein könnten, untersucht die Arbeitsgruppe „Risikoforschung und Sicherheitskulturen" unter Leitung von Prof. Dr. Renn.

Um das komplexe Verhältnis von Sicherheit, Risikoempfinden und Vertrauen in Institutionen und neue Technologien näher beleuchten zu können, ist eine Betrachtung der Grundmechanismen der Wahrnehmungsforschung und des Vertrauens erforderlich. Diese wird aber auch beeinflusst durch die Kompetenzen der Menschen in der Gesellschaft. Dazu ist es erforderlich, den Zusammenhang von Sicherheit und Kompetenz sowie seine Bedeutung näher zu beleuchten. Dies hat sich die Arbeitsgruppe „Bildung und Kompetenz" unter Leitung von PD Dr.-Ing. habil. Risch zum Ziel gesetzt. Sicherheit ist eine Kernkompetenz für die Wettbewerbsfähigkeit und die Nachhaltigkeit für Unternehmen und die Gesellschaft. Die ersten Untersuchungen dieser Arbeitsgruppe zur Verzahnung von Aus- und Weiterbildung auf dem Gebiet der ganzheitlichen Sicherheit konnten den Widerspruch zwischen dem Erkennen der Bedeutung von sicherheitsrelevantem Wissen und dem Aufbau eines effizienten Aus- und Weiterbildungsmanagements einschließlich des erforderlichen Forschungsbedarfs verdeutlichen.





Innerhalb dieser Unterarbeitsgruppen werden die jeweiligen Themenschwerpunkte vorangetrieben und diskutiert. Die ersten Ergebnisse aus den einzelnen Unterarbeitsgruppen wurden im Mai 2009 in einem Workshop zusammengeführt.

Jede der Unterarbeitsgruppen hat im Rahmen dieses Workshops ihre Ergebnisse in Form eines gemeinsamen Beitrags präsentiert und zudem Forschungsnotwendigkeiten aus der Perspektive der jeweiligen Unterarbeitsgruppe dargestellt. Ebenso haben ausgewählte Initiativen zum Thema Sicherheit (unter anderem „Deutschland sicher im Netz", DsiN, Kompetenzverbund „Sicherheit und Gesellschaft", Fraunhofer-Verbund „Verteidigungs- und Sicherheitsforschung") an dem Workshop teilgenommen und ihre Sicht auf das Thema Sicherheit sowie den Handlungsbedarf in ihrem Themengebiet bezüglich Sicherheit dargestellt. Diese Initiativen wurden im Vorfeld des Workshops aufgrund ihres Blickwinkels und ihres Arbeitsradius' aus den Ergebnissen einer deutschlandweiten Recherche ausgewählt.

Die genannten Standpunkte aus dem Themennetzwerk und den Initiativen wurden ausführlich im Workshop diskutiert und gehen im Ergebnis in diesen Band ein. Der vorliegende Band aus der Reihe „acatech diskutiert" ist damit ein erstes Diskussionsergebnis des Themennetzwerks Sicherheit. Die Beiträge veranschaulichen die Vielschichtigkeit des Begriffs „Sicherheit" sowie die entsprechenden Denkmodelle und Lösungsansätze. Alle Beiträge gehen davon aus, dass die begriffliche und wissenschaftliche Trennung von „Security" und „Safety" überwunden werden muss.





Die Notwendigkeit für diese Forderung kann anhand des Beispiels „Konzeptionierung eines Kinderplatzes" veranschaulicht werden. Bei der Neuanlage von Kinderspielplätzen treffen aus verschiedenen Richtungen Anforderungen für Safety und/oder Security aufeinander: Die Eltern der Kinder, die dort spielen sollen, legen Wert darauf, dass die Spielgeräte sicher sind, um das Verletzungsrisiko für die Kinder möglichst gering zu halten. Des Weiteren sollte aus ihrer Sicht der Spielplatz idealerweise von jedem Ort auf dem Spielplatz vollständig einsehbar sein, um eine Beaufsichtigung der Kinder zu erleichtern und es potenziellen Entführern oder anderen Verbrechern möglichst zu erschweren, unbemerkt in die Nähe der Kinder zu gelangen. Die an der Anlage des Spielplatzes beteiligte Kommune ist ebenso wie die Eltern daran interessiert, sichere Spielgeräte zur Verfügung zu stellen, um eventuellen Schadensersatzansprüchen und schlechter Publicity aus dem Weg zu gehen und den gesetzlichen Vorschriften Genüge zu tun. Der Gesetzgeber wiederum hat neben den eben erwähnten Sicherheitsanforderungen bezüglich der spielenden Kinder auch Anforderungen, die die Sicherheit der für den Aufbau und die Wartung der Geräte sowie der Grünflächen des Spielplatzes zuständigen Personen betreffen (Arbeitssicherheit). Neben den eben dargestellten Sicherheitsanforderungen können beispielsweise noch vonseiten der Passanten oder Autofahreren,





die Sorge haben, sie bzw. ihre Fahrzeuge könnten durch geworfene Bälle oder andere Spielgeräte gefährdet sein, oder diversen anderen Seiten vielfältige, sicherheitsrelevante Anforderungen eine Rolle spielen. Wie das Beispiel verdeutlicht, trennen die einzelnen Anforderungsquellen (Eltern, Passanten etc.) nicht zwischen „Safety"- und „Security"-Politik. In den Wissenschaften ist diese Trennung hingegen gängige Praxis, was eine ganzheitliche Betrachtung der Sicherheit des Systems deutlich erschwert. Eine solche Betrachtungsweise ist allerdings notwendig, um ein möglichst hohes Niveau an Sicherheit zu gewährleisten.

Sowohl bei der Entwicklung von neuen Technologien oder Produkten als auch bei der Erstellung von Gebäuden, Organisationen oder anderen Einrichtungen müssen also sowohl Safety- als auch Security-Aspekte berücksichtigt werden. Unternehmen der Zukunft benötigen infolgedessen eine Kernkompetenz auf dem Gebiet der Sicherheit. Dabei ist „Sicherheit" im umfassenden Sinne gemeint, sowohl als Sicherheit des Arbeitsschutzes als auch des Datenschutzes und des Personenschutzes, um nur einiges zu nennen. Während die Praxis schon nach dieser Integration der verschiedensten Schutzziele sucht, ist die Förderpolitik getrennt auf „Security" und „Safety" ausgerichtet. Dies muss überwunden werden.



Im vorliegenden Band sind eine Reihe von Forschungsansätzen skizziert, die dazu beitragen könnten, die Bereiche von „Safety" und „Security" zu überbrücken. So kann zum Beispiel die Taxonomie, basierend auf dem Systems Engineering oder neuen gesellschaftlichen Konzepten, die auf zu entwickelnden Kompetenzen sowie zu erstellenden Sicherheitskulturen basieren, neue Sicherheitsmodelle schaffen.

Neue Sicherheitskonzepte erfordern eine entsprechende Kommunikation, Motivation, Kompetenzentwicklung sowie das Schaffen gesellschaftlicher Voraussetzungen. Auf dieser Basis können dann Zukunftstechnologien durch eine Systemanalyse und ein Systemdesign mehr Sicherheit garantieren – wie dies gegenwärtig in der Praxis bereits umgesetzt wird. Welche offenen Fragestellungen bestehen bleiben, wird im letzten Abschnitt „Zur Umsetzung von Sicherheit in der Praxis" veranschaulicht.

Die Mitglieder des Themennetzwerks Sicherheit beabsichtigen, mit der Veröffentlichung dieser Beiträge in dem vorliegenden Band Vertreter aller gesellschaftlichen Schichten anzuregen, mit uns gemeinsam die zu lösenden Aufgaben im Themenfeld Sicherheit zu lokalisieren und in einem Folgeschritt zu priorisieren. Ziel ist es, darauf aufbauend als Ergebnis einer breiten nationalen und internationalen Diskussion Empfehlungen für die Verbesserung bestehender Sicherheitskonzepte entwickeln zu können, die ein gesellschaftliches Grundbedürfnis darstellen.



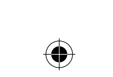



> THEMATISCHE UND BEGRIFFLICHE STRUKTURIERUNG DER AKTUELLEN SICHERHEITSFORSCHUNG











1 ZUKUNFTSTECHNOLOGIEN IN DER SICHERHEITS-FORSCHUNG

KLAUS THOMA/BIRGIT DREES/TOBIAS LEISMANN

1.1 EINLEITUNG: SICHERHEITSFORSCHUNG – WARUM?

Sicherheit ist nicht nur für jeden Menschen ein hohes persönliches Gut, das die Lebensqualität maßgeblich bestimmt; Sicherheit nimmt auch eine Schlüsselrolle in der politischen Stabilität und Rechtsstaatlichkeit eines Landes ein. Zuverlässig funktionierende Infrastrukturen wie Versorgungsketten, Verkehrswege, Kommunikations- und Bankensysteme bilden die Basis der modernen Industriegesellschaften. Die zunehmende Konzentration der Bevölkerung in Ballungszentren, die wachsende Vernetzung unterschiedlichster Lebensbereiche und -funktionen sowie der Übergang zu einer global vernetzten Informations- und Dienstleistungsgesellschaft vergrößern dabei die Verwundbarkeit durch Naturkatastrophen, Angriffe und Störungen vielfältiger Art.[1]

Sicherheitsforschung zielt darauf ab, diese Verwundbarkeiten zu erkennen, zu analysieren und Vorschläge bzw. Technologien zur Minderung oder Vermeidung der Risiken zu entwickeln, ohne in die Freiheit oder die Rechte des Bürgers einzugreifen. Dem Bericht des European Security Research Advisory Board (ESRAB) folgend, wird „Sicherheitsforschung" hier als Forschungsaktivität verstanden, die einen Beitrag zum Schutz vor ungesetzlichen oder vorsätzlich schädigenden Handlungen gegenüber Menschen, Infrastrukturen oder Organisationen leistet. Dazu zählt auch die Minimierung der Schädigungen, die sich aus solchen aktiven Eingriffen, aus Naturkatastrophen oder als Folge von Industrieunfällen ergeben. Strategien und Verfahren zur zeitnahen Wiederherstellung der normalen Funktion des Systems oder der Infrastruktur nach einer Störung sind ebenso Thema der Sicherheitsforschung.[2] Übergeordnetes und langfristiges Ziel muss der Aufbau einer widerstandsfähigen, fehlertoleranten und robusten Infrastruktur sein. Bisher ist die Sicherheitsforschung (noch) nicht als eigenständige Forschungsrichtung etabliert. Wissen und Kompetenzen aus Ingenieurs- und Naturwissenschaften sowie Geistes- und Sozialwissenschaften müssen systematisch zusammengeführt werden, um zu koordinierten Lösungen von Sicherheitsproblemen zu gelangen.[3]

Da die Sicherheitsforschung ein sehr breites wissenschaftliches und politisches Querschnittsthema darstellt, sind zu ihrer Entwicklung neue Ansätze notwendig. Während anfangs eine technologieorientierte Herangehensweise vorherrschte, die einzelne grundlegende Technologien für die Sicherheitsforschung losgelöst voneinander entwi-

1 Reichenbach et al. 2008.
2 European Communities 2006.
3 Beyerer 2007.





ckelte und erst im Engineering des Endprodukts zusammenführte und nutzbar machte („bottom-up"), setzt sich zunehmend ein szenarienorientierter Ansatz durch, der von Bedrohungs- und Gefährdungsszenarien ausgeht („top-down"). Dieser zweite Ansatz soll zu systematischen, sicherheitsrelevanten Gesamtkonzepten führen und, basierend auf Risikoanalysen, die Angreifbarkeit und Verwundbarkeit der betrachteten Systeme minimieren.[4] Wie im Folgenden dargestellt, kommt dem letztgenannten Ansatz sowohl auf europäischer Ebene als auch in der nationalen Umsetzung der Sicherheitsforschung eine große Bedeutung zu.

1.2 SICHERHEITSFORSCHUNG IN EUROPA UND IN DEN USA

1.2.1 ENTWICKLUNG DER SICHERHEITSFORSCHUNG IN EUROPA

Die immer komplexer verknüpften Strukturen der modernen Industriegesellschaft führen zu einer zunehmenden Verwundbarkeit unseres Lebensraums. Die weltweite Vernetzung der Infrastrukturen macht eine stärkere internationale Zusammenarbeit in der zivilen Sicherheit notwendig.[5] Daher hat die Europäische Union eine umfassende Strategie zum Aufbau einer europäischen Sicherheitsforschung entwickelt.

Als ein entscheidendes Instrument zur Entwicklung einer europäischen Verteidigungs- und Sicherheitspolitik werden Anstrengungen im Bereich der Forschung und Technologie gesehen. Im Auftrag der Europäischen Kommission erarbeitete eine „Group of Personalities" (GoP) Handlungsvorschläge zum Aufbau einer europäischen Sicherheitsforschung. Diese Empfehlungen umfassen unter anderem den Aufbau eines EU-geförderten Sicherheitsforschungsprogramms, das Aufheben der Trennung zwischen ziviler und wehrtechnischer Forschung, um vorhandene Technologien besser zu nutzen, die Schaffung eines European Security Research Advisory Board (ESRAB) zur Entwicklung der Inhalte des geplanten europäischen Sicherheitsforschungsprogramms und die Förderung eines Markts für sicherheits- und wehrtechnische Produkte.[6]

Durch den Start eines mit geringen finanziellen Mitteln ausgestatteten Vorläuferprogramms zum Sicherheitsforschungsprogramm, des „Preparatory Action for Security Research" (2004 bis 2006), konnte sich eine europäische Sicherheitsforschungsszene unter Beteiligung von Industrie, Behörden und Forschungseinrichtungen in Ansätzen entwickeln.[7]

Das ESRAB-Gremium wurde konstituiert und erarbeitete ein umfassendes Konzept für eine europäische Sicherheitsforschung.[8] Basierend auf diesem Konzept wurde das Thema Sicherheitsforschung mit einer Förderung von 1,4 Mrd. Euro für den Zeitraum

4 Beyerer/Geisler 2007.
5 Thoma 2008.
6 European Communities 2004.
7 Eine Beschreibung der 39 PASR-Forschungsprojekte einschließlich der End- und Zwischenergebnisse ist abrufbar unter: http://ec.europa.eu/enterprise/security/articles/article_2007-02-23_en.htm.
8 European Communities 2006.







von 2007 bis 2013 als neues Schwerpunktthema im spezifischen Programm „Zusammenarbeit“ in das 7. Forschungsrahmenprogramm der Europäischen Kommission aufgenommen.

Auf der Grundlage der Empfehlungen des ESRAB orientieren sich die Forschungsthemen des Rahmenprogramms inhaltlich an den vier Missionen:

- Schutz der Bürgerinnen und Bürger,
- Sicherheit von Infrastrukturen und Versorgungseinrichtungen,
- Schutz und Sicherung der europäischen Außengrenzen,
- Wiederherstellung der Sicherheit im Krisenfall.

Darüber hinaus werden noch die drei Querschnittsaktivitäten Integration und Interoperabilität von Sicherheitssystemen, Sicherheit und Gesellschaft sowie Koordinierung und Strukturierung der Sicherheitsforschung adressiert. Zur Erfüllung dieser Missionen werden bestimmte Fähigkeiten, sogenannte „Capabilities“ benötigt. Diese Fähigkeiten sind die Grundbausteine zur Technologiedefinition, denn sie stellen die kleinste Einheit von Technologien und Prozessen dar, die benötigt werden, um eine bestimmte Funktion, Aufgabe oder Operation durchzuführen.[9] Abbildung 1 veranschaulicht den fähigkeitsbasierten Ansatz der Sicherheitsforschung und zeigt unterschiedliche Forschungspfade auf, um die Ziele der Missionen zu erreichen.





Abbildung 1: Forschungspfade des EU-Sicherheitsforschungsprogramms nach ESRAB[10]

9 European Communities 2006.
10 European Commission 2008, S. 6.





Zur Fortführung der mit dem ESRAB begonnenen strategischen und inhaltlichen Ausrichtung des Sicherheitsforschungsprogramms wurde 2007 das European Security Research Innovation Forum (ESRIF) gegründet. In diesem Gremium beraten ausgewählte Experten der Mitgliedsstaaten aus Forschung, Industrie, dem Bereich öffentlicher und privater Endnutzer, der EU-Kommission sowie dem Europäischen Parlament und anderen europäischen Organisationen über die langfristige strategische Planung und die Ausrichtung der Sicherheitsforschung in Europa. Bis Ende 2009 soll das ESRIF eine gemeinsame Agenda für Sicherheitsforschung aufstellen, die Empfehlungen enthalten wird zu den Themen „verbesserte Sicherheit von Infrastrukturen", „Kampf gegen das organisierte Verbrechen und den Terrorismus", „Wiederherstellung der Sicherheit in Krisenzeiten" sowie eine „Verbesserung der Grenzüberwachung und -kontrolle".

1.2.2 NATIONALE SICHERHEITSFORSCHUNGSPROGRAMME IM VERGLEICH

1.2.2.1 DEUTSCHLAND

Auch auf nationaler Ebene wird auf die veränderte Sicherheitssituation reagiert. In Deutschland wurde das Thema Sicherheit als eines von 17 Zukunftsfeldern in die Hightech-Strategie der Bundesregierung aufgenommen, um so sicherheitsrelevante Entwicklungen im Bereich Forschung und Technologie schwerpunktmäßig zu fördern.[11] Sicherheitsforschung wird dadurch erstmals als Thema von herausragendem nationalen Interesse definiert. Um die Hightech-Strategie umzusetzen und um die systematische und strategische Forschung für die zivile Sicherheit zu stärken, wurde ein nationales Sicherheitsforschungsprogramm entwickelt, das gleichzeitig mit dem Sicherheitsforschungsprogramm im 7. Rahmenprogramm der EU anlief. In Deutschland wird die Entwicklung von neuartigen Sicherheitslösungen damit erstmals ressortübergreifend, d. h. in Abstimmung mit allen Bundesministerien, gefördert. Das Programm „Forschung für die zivile Sicherheit" ist auf den Schutz der Bürger gegen Bedrohungen durch organisierte Kriminalität, Terrorismus und die Folgen von Naturkatastrophen und Großunfällen ausgelegt. Der Schutz der sogenannten „kritischen Infrastrukturen" wie zum Beispiel Energieversorgungssysteme, Verkehrsnetze und Telekommunikationsstrukturen ist dabei ein zentrales Thema. Für den Zeitraum von 2007 bis 2010 ist dieses Programm mit 123 Mio. Euro ausgestattet.[12] Da es bisher keinen derartigen Forschungsschwerpunkt gab, müssen hier viele Verfahren, Strategien, Ziele und auch Märkte erst entwickelt werden, beziehungsweise vorhandenes Wissen sowie verfügbare Entwicklungen und Technologien müssen für die Sicherheitsforschung genutzt und angewandt werden.

Die Umsetzung erfolgt in Form von Verbundprojekten in zwei Programmlinien. Programmlinie 1 umfasst die „Szenarienorientierte Sicherheitsforschung". Ausgangspunkte sind nicht spezielle technische Problematiken, sondern konkrete Bedrohungssituationen.

---

[11] BMBF 2006.
[12] BMBF 2007.







Dadurch sollen alle Disziplinen aus Technik, Natur-, Geistes- und Sozialwissenschaften, die für eine Erarbeitung umsetzungsfähiger Sicherheitslösungen notwendig sind, eingebunden werden. Schwerpunkte sind Schutz und Rettung von Menschen, Schutz von Verkehrsinfrastrukturen, Schutz vor Ausfall von Versorgungsstrukturen und Sicherung der Warenketten. In der Programmlinie 2 wird die Erforschung von Querschnittstechnologien in „Technologieverbünden" verfolgt. Innovative Systeme werden aus bestehenden und neuen Technologien anwendungsnah entwickelt. Dazu zählen die Technologien zur raschen und mobilen Erkennung von Gefahrstoffen, zur Unterstützung von Sicherheits- und Rettungskräften, zur Mustererkennung und zur schnellen und sicheren Personenidentifikation durch Biometrie. Integraler Bestandteil des Programms ist die Betrachtung gesellschaftlicher und juristischer Dimensionen der Forschung. Dabei wird unter anderem kritischen Fragen zur Ethik, zur Akzeptanz von neu entwickelten Sicherheitslösungen oder zu deren rechtlichen Grundlagen nachgegangen.

Die Fraunhofer-Gesellschaft hat frühzeitig die Bedeutung der Sicherheitsforschung erkannt. Im Rahmen eines Portfolio-Prozesses wurde die Sicherheitsforschung als eines von zwölf langfristigen Innovationsthemen identifiziert. Die Fraunhofer-Innovationsthemen zeichnen sich durch ein herausragendes Innovationspotenzial, hohen Forschungsbedarf, Marktnähe und Fokussierung auf Fraunhofer-Kompetenzen aus.[13] Als Schwerpunkte wurden die Themen Sicherheit in Information und Kommunikation (Sicherheit durch IT-Systeme, IT-Sicherheit, Kommunikation für mehr Sicherheit), Krisen- und Katastrophenmanagement (Wiederherstellung der Sicherheit im Krisenfall), multisensorische Detektion und Identifikation für Gefahrenaufklärung und Überwachung, Detektion und Monitoring von Gefahrstoffen, Robotik, Schutzsysteme und Werkstoffe sowie Risikomanagement abgeleitet.[13]

Das nationale Sicherheitsforschungsprogramm ist passfähig zum 7. Forschungsrahmenprogramm und stellt daher eine wichtige Umsetzung und Ergänzung der sicherheitsrelevanten europäischen Forschung dar. Durch die Initiierung des nationalen Forschungsprogramms wird den deutschen Akteuren in Industrie und Forschung die Chance geboten, Kompetenzen und Know-how zu erwerben und sich auf dem europäischen und internationalen Markt für Sicherheitsprodukte und -technologien zu positionieren. Als ein zentrales Wissenschaftsforum für die Sicherheitsforschung hat sich die Konferenz „Future Security" etabliert.[14]

1.2.2.2 FRANKREICH

Die französische Sicherheitsforschung wird seit 2006 im Rahmen des nationalen Programms „Concepts, Systèmes et Outils pour la Securité Globale" (CSOSG) gefördert. Dieses Programm soll die Grundlage für die Forschung im Bereich der inneren Sicherheit bereitstellen und beinhaltet eine jährliche Fördersumme von ca. 11 Mio. Euro.[15] Gemein-

13 Buller/Thoma 2006.
14 Thoma 2008; siehe auch: www.vvs.fraunhofer.de.
15 ANR 2009.





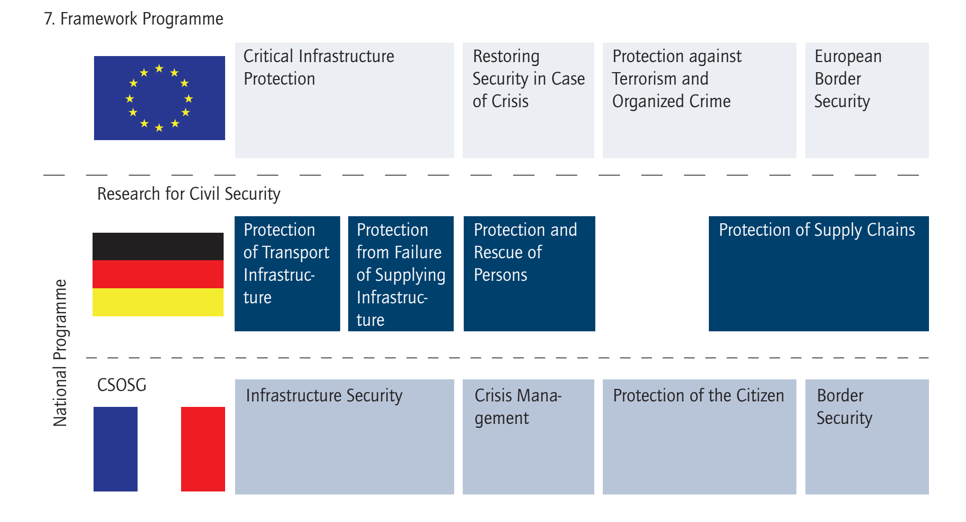


schaftlich gesteuert durch das französische Innenministerium (Ministère de l'Intérieur, de l'Outre-Mer et des Collectivités Territoriales), das Verteidigungsministerium (Ministère de la Défense) und die nationale Forschungsagentur (Agence Nationale de la Recherche, ANR) soll sowohl die projektbasierte Entwicklung sicherheitsrelevanter Technologien und Entwicklungen unterstützt als auch die französische Sicherheitsforschung für den europäischen Wettbewerb gestärkt werden.

Die Ausschreibungen zur Projektförderung innerhalb des CSOSG sind thematisch in vier Themengebiete unterteilt: Schutz der Bürger, Schutz von Infrastrukturen und Netzwerken, Grenzsicherheit und Krisenmanagement.[16] Damit lassen sich hier die übergeordneten Missionen, die der Zielformulierung in der europäischen Sicherheitsforschung dienen, klar in der nationalen Umsetzung wiederfinden (vgl. Abbildung 2).

Abbildung 2: Umsetzung der vier Missionen der europäischen Sicherheitsforschung in Schwerpunktthemen des deutschen und des französischen Sicherheitsforschungsprogramms. Die starke Ausrichtung des französischen Programms an dem europäischen wird deutlich.





Die Ausrichtung des französischen Programms an den europäischen Missionen zeigt Wirkung auf den Erfolg französischer Sicherheitsforscher im europäischen Vergleich: Im Jahr 2007 gingen 13 Prozent der Förderverträge (und damit 21 Mio. Euro Fördermittel)



[16] ANR 2009.





des Sicherheitsforschungsprogramms im 7. EU-Rahmenprogramm an französische Partner. Damit lag Frankreich auf dem vordersten Platz vor Großbritannien und Deutschland.[17]

Durch gemeinsame Ausschreibungen in der Sicherheitsforschung wird die Förderung der bilateralen Forschungszusammenarbeit Deutschlands und Frankreichs gestärkt und damit eine Entwicklung hin zu einer stärkeren europäischen Zusammenarbeit vorangetrieben. Beispielhaft zu nennen ist hier die nationale Förderausschreibung zur „Sicherheit der Warenkette" im Jahr 2009, die für bilaterale Verbundprojekte geöffnet wurde.[18]

1.2.3 THEMEN DER SICHERHEITSFORSCHUNG IN DEN USA

Ein Blick nach Nordamerika soll exemplarisch zeigen, welche sicherheitsrelevanten Themen außerhalb von Europa von Bedeutung sind. Dazu wird hier eine Studie des Nationalen Forschungsrats der USA zur Rolle von Wissenschaft und Technologie im Kampf gegen den Terrorismus herangezogen, die 2001 aufgrund der gewandelten Bedrohungssituation initiiert wurde.[19]

Der Bericht „Making the Nation Safer" charakterisiert die Spannweite der Bedrohungen der nationalen Sicherheit und benennt wichtige Möglichkeiten, wie durch langfristige Forschung und Entwicklung gegenwärtige und zukünftige Risiken minimiert werden können. Terroristische Anschläge mit nuklearen, radiologischen, toxischen oder explosiven Gefahrstoffen können auf Ziele wie die Gesundheit von Mensch und Tier, Informationstechnologien, Energiesysteme, Transportsysteme, Städte und bauliche Infrastruktur oder komplexe, untereinander verbundene und voneinander abhängige Systeme ausgerichtet sein. Solche Anschläge können auch weitreichende Auswirkungen auf Systeme und Infrastrukturen haben, die in enger Wechselbeziehung zu dem eigentlichen Ziel eines Anschlags stehen.



Aus diesen Bedrohungsszenarien werden Empfehlungen für Forschung und Entwicklung zur Erhöhung der Sicherheit abgeleitet. So sollen Risiko- und Schadensanalysen zu kritischen Infrastrukturen und Versorgungs- bzw. Transportsystemen helfen, sowohl Schwachstellen als auch Interdependenzen zu identifizieren. Dazu gehört auch die Modellierung verschiedener Anschlagsszenarien oder die Untersuchung von Ausbreitungscharakteristika gefährlicher chemischer oder biologischer Substanzen. Ebenso wie in Europa wird das zentrale Ziel verfolgt, robuste Systeme und Infrastrukturen zu entwickeln, die widerstandsfähig gegen terroristische Angriffe jeglicher Art und gegen Naturkatastrophen sind. Eine Schlüsselrolle in der Gefahrenabwehr nimmt auch hier

[17] Intelligence online 2008.
[18] BMBF 2009a.
[19] Committee on Science and Technology for Countering Terrorism 2002.







die Früherkennung von Bedrohungen (zum Beispiel durch versteckte Waffen) und die echtzeitnahe Detektion von Gefahrstoffen ein. Sensoren, die zuverlässig konventionelle Explosivstoffe und unkonventionelle chemische, biologische und radioaktive Stoffe detektieren können, wird auf beiden Seiten des Atlantiks eine entscheidende Bedeutung zugemessen. Auch bei Maßnahmen zur besseren Unterstützung von Rettungs- und Einsatzkräften vor (zum Beispiel durch Simulationssoftware) und während eines Einsatzes (Verbesserung der Informations- und Kommunikationssysteme) wird Entwicklungsbedarf gesehen. Eine schnelle Wiederherstellung von Transport- und Versorgungssystemen soll zur Vermeidung von Kaskadeneffekten beitragen. Forschungsbedarf besteht auch zu Aspekten der Dekontamination nach einem Schadensereignis.

Das Department of Homeland Security hat in einer Broschüre die Technologien zusammengestellt, die aus Sicht des Ministeriums für die zivile Sicherheit dringend erforderlich sind.[20] Diese werden unterteilt in die Bereiche Grenzschutz, Frachtsicherheit, chemische und biologische Abwehr, Internetsicherheit, Verkehrssicherheit, Counter-IED (Improvised Explosive Device), Krisenmanagement, Austausch von Informationen, Infrastruktursicherheit, Zusammenarbeit, maritime Sicherheit und das Screening von Personen. Eine repräsentative Liste der benötigten Technologien gibt Abbildung 3 wieder.

Die Ausführungen zeigen, dass es eine große Überlappung der Schwerpunktthemen im Bereich der Sicherheitsforschung in Europa und den USA gibt.



Abbildung 3: Prioritäre Technologien in der US-Sicherheitsforschung[20]

BORDER SECURITY	– Detection, tracking, and classifying of all threats along the terrestrial and maritime border – Improved ballistic protection via personal protective equipment – Non-destructive tools that allow the inspection of hidden or closed compartments – Ability for law enforcement officers to assure compliance of lawful orders using non-lethal means – Ability for law enforcement personnel to quickly identify the origin of gunfire and classify the type of weapon fired – Improved analysis and decision-making tools that will ensure the development and implementation of border security initiatives – Non-lethal compliance measures for vehicles, vessels, or aircraft, allowing safe interdiction by law enforcement personnel
CARGO SECURITY	– Improved screening and examination by non-intrusive inspection – Increased information fusion, anomaly detection, Automatic Target Recognition capability – Detect and identify WMD materials and contraband – Capability to screen 100 percent of air cargo

[20] DHS 2008.



CARGO SECURITY	– Track domestic high-threat cargo – Positively ID cargo and detect intrusion or unauthorized access – Reliable container seal security/detect intrusion devices
CHEMICAL-BIOLOGICAL DEFENSE	– Improved Chemical-Biological Forensic Analysis capability – Handheld rapid biological and chemical detection systems – Policy net assessments to provide fresh perspectives on fundamental elements of the national biodefense strategy – Detection paradigms and systems for improved, emerging, and novel biological threats – Tools to detect and mitigate animal disease breakouts – National-scale detection architectures and strategies to address outdoor and indoor (for example, highly trafficked transportation hubs) and critical infrastructure – Consequence assessment of attacks on chemical facilities and Chemical-Biological attacks on other critical infrastructure – Integrated CBRNE Sensor Reporting capability – Improved tools for integrated CBRN Risk Assessment – Incident characterization capability for response and restoration – Mechanisms to independently evaluate and validate commercially developed assays for the first-responder community to be public health actionable – Tools for sampling, rapidly detecting, and identifying in the field illegal products, including high-consequence pathogens and toxins that threaten agriculture and the food industry
CYBER SECURITY	– Secure Internet protocols, including standard security methods – Improved capability to model the effects of cyber attacks – Comprehensive next-generation network models – Composable and scalable secure systems – Technologies and standards for managing the identities, rights, and authorities used in an organization's networks – Information-system insider-threat detection models and mitigation technologies – Analytical techniques for security across the IT system-engineering lifecycle – Process Control Systems (PCS) security
TRANSPORTATION SECURITY	– Technologies to screen people for explosives and weapons at fixed aviation and mass-transit checkpoints – System solutions for explosives detection in checked and carried bags – Capability to detect homemade or novel explosives – Optimized canine explosive detection capability – Technologies for screening air cargo for explosives and explosive devices
COUNTER IED	– Capability to detect domestic use vehicle-borne improvised explosive devices (VBIEDs) – Capability to assess, render safe, and neutralize explosive threats – Capability to detect person-borne IEDs from a standoff distance – Capability of inerting common explosives or making them less sensitive to initiation







COUNTER IED	– Techniques to track the origin of explosives and bomb components used in domestic IEDs – Capability to mark explosives material to improve the detection of IED – Low-cost and practical approaches to protect urban structures and occupants from VBIED attacks – Protective measures to reduce damage and prevent catastrophic failure of high-consequence infrastructure assets subjected to IED attacks – Models for the prediction of blast effects that take into account the diversity and variability of construction in urban settings – Affordable blast-, fragment-, and fire-resistant materials – Rapidly deployable blast-mitigation concepts for rapid threat response or temporary protection – Tools to rapidly assess damaged structures – Techniques and tools to stabilize damaged structures and prevent their collapse – Capability to predict the threat of an IED attack – Increased capability at vehicle or pedestrian ports of entry and border crossings to identify person born IED threats – Enhanced capability for local officials to communicate understandable and credible IED warnings and instructions to the public
INCIDENT MANAGEMENT	– Integrated modeling, mapping, and simulation capability – Personnel monitoring (emergency responder 3-D locator system) capability – Personnel monitoring (physiological monitoring of firefighters) capability – Incident management enterprise system – Logistics management tool
INFORMATION SHARING	– Data fusion from law enforcement, intelligence partners, and other sensors to support the common operating picture (COP) – Management of user identities, rights, and authorities – Distribution of intelligence products – Information sharing within and across sectors on terrorist threats – Improvement of situational awareness and decision support – Situational awareness between U.S. Coast Guard and partners – Predictive analytics – Protection of U.S. citizen personal data – Improved cross-agency reporting of suspicious activity
INFRASTRUCTURE PROTECTION	– Analytical tools to quantify interdependencies and cascading consequences as disruptions occur across critical infrastructure sectors – Effective and affordable blast analysis and protection for critical infrastructure, and an improved understanding of blast-failure mechanisms and protection measures for the most vital critical infrastructures and key resources (CI/KR) – Advanced, automated, and affordable monitoring and surveillance technologies – Rapid mitigation and recovery technologies to quickly reduce the effect of natural and manmade disruptions and cascading effects – Critical utility components that are affordable, highly transportable, and provide robust solutions during manmade and natural disruptions







INTEROPERABILITY	– Accelerate the development of Project 25 and Internet Protocol (IP) interfaces – Standardize, pilot, and evaluate emergent wireless broadband data technologies and applications – Develop message interface standards that enable emergency-information sharing and data exchange – Develop complementary test procedures – Provide seamless access to voice and data networks, using a unified communications device – Perform interoperability compliance testing on emergency response communications devices and systems
MARITIME SECURITY	– Wide-area surveillance from the coast to beyond the horizon, including port and inland waterways, for detection, ID & tracking – Data fusion and automated tools for command center operations – Improve the capability to continuously track contraband on ships or containers – Develop improved ballistic personal protective equipment for officers – Vessel compliance through less-lethal compliance – Ability for law-enforcement personnel to detect and identify narcotics, chemical warfare agents, toxic industrial chemicals, explosives, and contraband materials
PEOPLE SCREENING	– Systematic collection and analysis of information related to understanding a terrorist group's intent to engage in violence – Real-time detection of deception or hostile intent – Capability in real time for positive verification of an individual's identity, using multiple biometrics – Capability for secure, non-contact electronic credentials; contactless readers or remote interrogation technologies for electronic credentials – Mobile biometrics screening capabilities, including handheld, ten-fingerprint-capture, environmentally hardened, wireless, and secure devices – High-speed, high-fidelity ten-print capture capability – Rapid DNA testing to verify family relationships during interviews for the disposition of benefits – Remote, standoff biometrics detection for identifying individuals at a distance






1.3 VOM FORSCHUNGSPROGRAMM ZU MARKTFÄHIGEN TECHNOLOGIEN

Das oberste Ziel aller Bemühungen in der Sicherheitsforschung ist, die Sicherheit der Bürgerinnen und Bürger zu gewährleisten. Es geht also zentral um die Fähigkeit, Bedrohungen und Gefahren abzuwehren oder zu minimieren bzw. Krisen zu bewältigen. Wie oben bereits beschrieben, definieren die nationalen und übergeordneten Programme dafür die wichtigen, zielführenden Themen. Doch mittels welcher konkreten Technologien können diese Fähigkeiten erreicht werden? An welchen Entwicklungen und Forschungsansätzen wird derzeit gearbeitet? Da die Entwicklung von Technologien wesentlich von Marktpotenzialen gelenkt wird, stellt sich auch die Frage, welche Sicherheitstechnologien kommerziellen Nutzen versprechen.

Um der Beantwortung dieser Fragen näher zu kommen, sollen im Folgenden zwei Ansätze verfolgt werden. Zunächst werden, ausgehend von den geförderten Forschungsprojekten, die Schwerpunkte der Technologieentwicklungen aufgezeigt. Daher werden hier hauptsächlich Technologien miteinbezogen, die eigens für den Bereich der zivilen Sicherheit entwickelt werden. Andere Entwicklungen, deren Nutzen für diese Disziplin vielleicht erst nachträglich erkannt wird, bleiben unberücksichtigt. Die zweite Herangehensweise stützt sich auf aktuelle Marktanalysen, die einen Hinweis auf die Entwicklung des Bedarfs an Sicherheitstechnologien geben sollen.




1.3.1 GEFÖRDERTE TECHNOLOGIEENTWICKLUNGEN

Der ESRAB-Report benennt eine Reihe von konkreten Technologiefeldern, die von entscheidender Bedeutung sind, um zukünftig den wichtigsten Sicherheitsanforderungen gerecht zu werden (vgl. Abbildung 4). Hierzu zählen viele sogenannte Schlüsseltechnologien, die in viele verschiedene Systeme integriert werden können bzw. müssen, um die Sicherheit in bestimmten Risikoszenarien zu gewährleisten. Einen hohen Stellenwert haben dabei beispielsweise Informations- und Kommunikationstechnologien, Systeme zur Entscheidungsunterstützung und Sensortechnologien. Diese Liste gibt den „top-down"-Ansatz des europäischen Entwicklungsprozesses der Sicherheitsforschung wieder. Die umfangreiche Anzahl der Technologiefelder wird aber nicht weiter priorisiert; dies geschieht erst mit der Veröffentlichung von Ausschreibungen und der nachfolgenden Auswahl von Verbundprojekten zur Förderung.





Abbildung 4: Prioritäre Technologiefelder nach Technologiebereichen (dem ESRAB Report entnommen)[21]

TECHNOLOGY DOMAIN	PRIORITY TECHNOLOGY AREAS
Signal & information technologies	data collection/data classification, image/pattern processing technology, data and information management technology (DB etc.)
Artificial intelligence and decision support	text-mining/data-mining, IKBS/AI/expert techniques, knowledge management, modelling and simuation, optimisation and decision support technology
Sensor equipment	cameras, radar sensor equipment, CBRN sensors (in particular biological and chemical threat detection technologies), passive IR sensors equipments
Sensor technologies	hyperspectral/multispectral sensors, hyperspectral/multispectral processing, IR sensor technologies, Terahertz sensors, acoustic sensors – passive, optical sensors technologies
Communication equipment	reconfigurable communications, mobile secured communications, information security, network supervisor, network and protocol independent secured communications, communications network management and control equipment, secured, wireless broadband data links for secured communications, protection of communication networks against harsh environment
Human sciences	human behaviour analysis and modeling, population behaviour, human factors in the decision process, teams, organisations and cultures
Information security technologies	encryption and key management, data-mining, access control, filtering technologies, authentication technologies, encryption technologies (cryptography)
Computing technologies	protocol technology, SW architectures, secure computing techniques, high performance computing, high integrity and safety critical computing, software engineering
Information warfare/ intelligence systems	infrastructure to support information management and dissemination, cyber security policy management tools, optimisation, planning and decision support systems
Scenario and decision simulation	impact analysis concepts and impact reduction, advanced human behaviour modeling and simulation, simulation for decision making (real time simulation), structures vulnerability prediction, evacuation and consequence management techniques, mission simulation
Information systems	infrastructure to support information management and dissemination, cyber security policy management tools, optimization, planning and decision support systems
Navigation, guidance, control and tracking	RFID tags, tracking, GPS, radionavigation, direction finding and map guidance, bar code based tracing
Forensic technologies – biometry	fingerprints recognition (digital fingerprints), facial recognition, iris/retina, voice, handwriting, signature reconnaissance



[21] European Communities 2006, S. 50.





Integrated platforms	UAVs (air/land/sea), lighter than air platforms, surveillance and navigation satellites
Survivability and hardening technology	EMC evaluation and hardening, smart clothes and equipment, anti-blast glasses/concretes, critical buildings specific architectures, blast and shock effects
Electronic authentication	electronic tagging systems, smart cards
Biotechnology	rapid analysis of biological agents and of human susceptibility to diseases and toxicants, decontamination techniques, water testing and purification techniques, food testing and control techniques
Simulators, trainers and synthetic environments	virtual and augmented reality, tactical/crew training systems, command and staff training systems, synthetic environments
Chemical, biological and medical materials	chemical and biological detection systems
Space systems	earth observation (image and communications)
Light and strong materials, coatings...	light materials for human protection, smart textiles, light materials for site protection, self-protective and explosive resistant material technology, corrosion reduction
Energy generation storage and distribution	electrical generators, electrical batteries, energy distribution, microenergy technologies



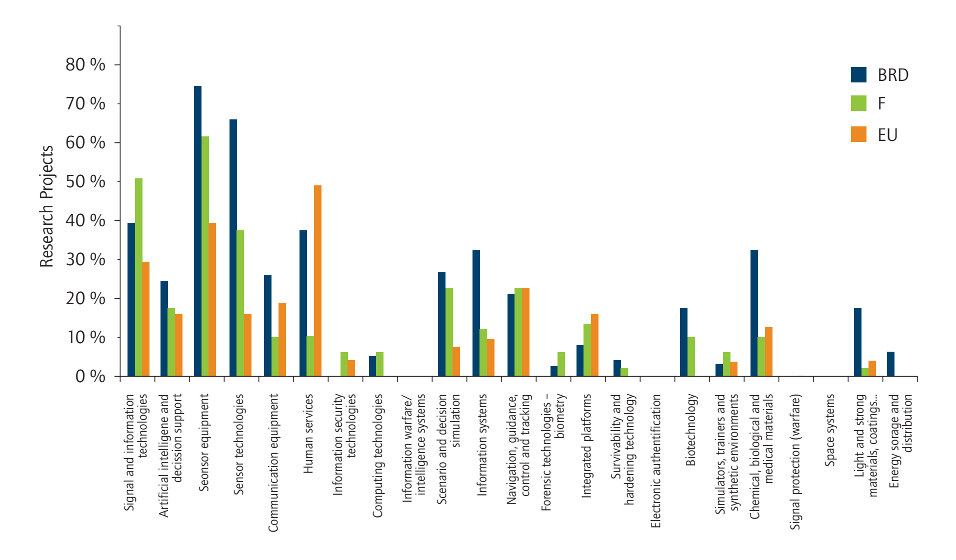

Um aus der gegenwärtigen Sicherheitsforschung ein Bild über die Technologien der Zukunft zu gewinnen, wurden die laufenden Forschungsprojekte des deutschen, französischen und europäischen Programms den ESRAB-Technologien zugeordnet (Abbildung 5). Dargestellt ist der Anteil der Projekte, die sich mit einer Technologie beschäftigen; ein Projekt kann dabei auch mehrere Technologien erforschen. Daraus ergibt sich ein „bottom-up"-Ansatz zur Priorisierung der Technologiefelder. Wichtig hierbei ist, dass die Grafik lediglich eine erste Momentaufnahme der aktuell geförderten Projekte in den Sicherheitsforschungsprogrammen wiedergibt. Dieser Prozess hat jedoch gerade erst begonnen. Während das Programm „Forschung für die zivile Sicherheit" der deutschen Bundesregierung noch bis 2010 läuft, hat das europäische Sicherheitsforschungsprogramm eine Laufzeit bis 2013. Daher stehen noch zusätzliche Ausschreibungen aus, die weitere wichtige Themenfelder adressieren und entsprechend zukunftsträchtige Technologien generieren werden. Abbildung 5 zeigt dennoch, dass die verschiedenen Forschungsprogramme zu einer ähnlichen Verteilung der Projekte führen, trotz der unterschiedlichen Art, die Ausschreibungen zu gestalten. So ist der Anteil der Projekte, die beispielsweise „Signal and Information Technologies" entwickeln, in Frankreich zwar am höchsten (50 Prozent), aber in Deutschland und der EU mit knapp 40 bzw. 30 Prozent auch nicht unerheblich. Andererseits ist die Entwicklung von „Integrated Platforms" bei allen Programmen mit maximal 15 Prozent der Projekte eher spärlich ausgeprägt.





Wo Themenbereiche in der aktuellen Forschung unterrepräsentiert sind, müssen die Forschungsprogramme nachsteuern, um das gesamte Spektrum der benötigten Entwicklungen abdecken zu können. Zu berücksichtigen ist aber, dass in einigen Themenbereichen bereits vielfältig nutzbare Technologien entwickelt worden sind (zum Beispiel Electronic ID, Smart Cards) und dass auch andere Forschungsprogramme (Informations- und Kommunikationstechnologien, Energie, Weltraum) sicherheitsrelevante Themen und Technologiefelder fördern.

Abbildung 5: Vergleich der projektbasierten Forschungs- und Entwicklungstätigkeiten Deutschlands (39 Verbundprojekte), Frankreichs (49 Projekte) und auf europäischer Ebene (31 Projekte). Die Technologieentwicklungen sind bezogen auf die Gesamtzahl der geförderten Projekte (kategorisiert nach den im ESRAB herausgestellten prioritären Forschungsfeldern, Forschung an mehreren Technologiefeldern in einem Projekt möglich, Stand: 1.3.2009.)



1.3.1.1 SENSORTECHNOLOGIEN

Besonders stark werden in allen drei Forschungsprogrammen bisher Sensorausrüstung und -technologien gefördert. Deutschland beteiligt sich an deren Entwicklung in herausragendem Maße: Von den insgesamt 39 vom BMBF geförderten Verbünden beschäftigen sich 29 unter anderem mit diesen Aspekten.[22] Sensortechnologien wird somit eine wichtige Rolle in der Sicherheitsforschung zuerkannt. Grund dafür sind wohl das sehr breite Einsatzspektrum und der erwartete hohe Nutzen durch den Einsatz von automatisierbaren, multisensorischen und mobilen Sensorsystemen.[23] Ein Schwerpunkt

[22] Stand: 1. März 2009.
[23] Thoma in: BMBF 2008.







der gegenwärtigen Sensorforschung liegt, vorangetrieben durch eine Förderbekanntmachung des BMBF im Jahr 2008, bei der Entwicklung von Detektoren von chemischen, explosiven und biologischen Gefahrstoffen.[24] Ein zentrales Forschungsfeld ist die Probenentnahme und die schnelle Detektion und Analyse von Gefahrstoffen vor Ort (auch aus großer Entfernung). Technologische Lösungen zur Detektion von hochtoxischen oder gefährlichen Substanzen in der Luft sind beispielsweise Systeme, mit denen Gasspuren angereichert und mittels gaschromatografischer Trennung über verschiedene Sensoren analysiert werden können. Biologische Breitbandsensoren zur Trinkwasserüberwachung oder portable Diagnostiksysteme mit Spektrometern zum Aufspüren und Erkennen bakterieller Kontaminationen sind Beispiele aktueller Entwicklungsansätze zur Detektion biologischer Gefahrstoffe. In Zukunft sollen Sensortechniken auch deutlich stärker zur Unterstützung von Einsatzkräften genutzt werden. Beispielsweise können energieautarke Funksensornetze Auskünfte über die Resttragfähigkeit von Bauwerken nach einer Explosion geben,[25] sodass Einsatzkräfte einsturzgefährdete Bereiche meiden können. Ein weiteres Forschungsfeld ist die Entwicklung innovativer Schutzanzüge mit integrierten Sensoren, die ein sicheres und zielgerichtetes Handeln der Einsatzkräfte unterstützen, unter anderem durch eine Überwachung der Vitalparameter der Einsatzperson, Messung der Umgebungsbedingungen oder durch integrierte Kommunikationssysteme mit Ortungsmöglichkeiten.[26] Darüber hinaus können Drohnen mit miniaturisierter Onboard-Sensorik zur Lageaufklärung aus der Luft beitragen.

Die gegenwärtige intensive Forschung im Bereich der Sensortechnologien wird in Zukunft einen verstärkten Einsatz von Sensoren in allen Bereichen der Sicherheit ermöglichen. Insbesondere die Nutzung von Multisensorsystemen und von vernetzten Sensorsystemen wird zu vielfältigen neuen Produkten und Anwendungen führen, was man in anderen Bereichen (zum Beispiel in der KFZ-Motorsensorik oder der Unterhaltungselektronik mit Mobiltelefonen voller Sensorik) schon heute beobachten kann.

Zukunftsweisende Technologien und vielversprechende Sicherheitslösungen sind aber auch in vielen anderen, in den Forschungsprogrammen bislang weniger stark berücksichtigten Themenfeldern zu erwarten. Daher ist es von entscheidender Bedeutung, dass die Sicherheitsforschung ebenso intensiv auch an andere prioritäre Forschungsfelder herangeht.

1.3.1.2 RISIKO- UND GEFÄHRDUNGSANALYSEN

Simulationen spielen bei der Abschätzung der Wahrscheinlichkeit und des Ausmaßes eines terroristischen Angriffs oder einer Naturkatastrophe eine grundlegende Rolle. Solche Risiko- und Gefährdungsanalysen sollten Ausgangspunkt für die Einführung von Sicherheitsmaßnahmen sein, um so gezielt und effizient die zivile Sicherheit zu erhöhen. Einige solcher Software Tools und Programme sind bereits im Einsatz und bilden

[24] BMBF 2008.
[25] Riedel/Schäfer 2008.
[26] BMBF 2009b.







in zunehmend größerer Detailtreue die reale Welt ab; damit erlauben sie auch immer genauere Prognosen zu den Folgen beispielsweise eines terroristischen Anschlags mit Sprengstoff.[27]

Forschungs- und Entwicklungsbedarf besteht bei Simulations- und Optimierungsinstrumenten zur Unterstützung von Entscheidungsprozessen im Krisenfall. Nur bei Kenntnis der genauen Gefahren können geeignete Gegenmaßnahmen ergriffen werden. Die Simulation von Schlüsselfaktoren wie die Brand- oder Gefahrstoffausbreitung, Resttragfähigkeit von Gebäuden oder Evakuierungssituationen von Personenströmen trägt maßgeblich zum optimalen Einsatz von Rettungskräften bei. Verfahren zur automatischen Lagebewertung ebenso wie Systeme, die in Gefahrensituationen automatisch optimale Entscheidungen treffen, können die kritische Zeitspanne bis zur Einleitung von Maßnahmen zur Wiederherstellung der Sicherheit entscheidend verkürzen.

1.3.1.3 SCHUTZ KRITISCHER INFRASTRUKTUREN

Die Entwicklung von baulichen Maßnahmen zum Schutz kritischer Infrastrukturen zielt vorrangig auf eine Erhöhung des Schutzes vor terroristischen Angriffen mit Explosivstoffen oder vor natürlichen Extremereignissen. Laufende Forschungsprojekte auf nationaler Ebene adressieren vor allem die Sicherheit von Verkehrsinfrastrukturen. In ihnen wird beispielsweise, basierend auf einer Risikoanalyse, die Implementierung von baulichen Schutzmaßnahmen an Flughäfen analysiert. Als weitere Innovationen sind unter anderem die Verwendung von energieabsorbierenden Materialien zur Ummantelung von Gebäuden, druckwellenbeständige Fassadenelemente oder die Entwicklung brandbeständiger ultrahochfester Betone und deren Verwendung zur Fertigung von Bauteilen zu nennen. Auch im Bereich des baulichen Schutzes sind weitere zukunftsweisende Entwicklungen zu erwarten, da im nächsten Aufruf zum Themenfeld Sicherheit im 7. EU-Rahmenprogramm mit entsprechenden Ausschreibungen zu rechnen ist. Dies betrifft zum einen die umfassende Maßnahmenrealisierung zur Erhöhung der Widerstandsfähigkeit von Verkehrsknotenpunkten (Flughäfen, Bahnhöfe, Häfen etc.) und zur Realisierung der dazugehörigen Infrastruktur im Rahmen eines Demonstrationsprojekts. Zum anderen sollen robuste, widerstandsfähige und gleichzeitig kostengünstige Materialen, Bauteile und Bauweisen für den Einsatz in kritischen Infrastrukturen entwickelt werden.



Eine sichere Energieversorgung ist in unserer technisierten Welt von entscheidender Bedeutung und stellt ein wichtiges Zukunftsthema in der Sicherheitsforschung dar. Sowohl die Informations- und Kommunikationssicherheit kritischer Energieinfrastrukturen als auch der bauliche Schutz, beispielsweise von öffentlichen Gebäuden, sind nicht nur wichtig für die wirtschaftliche Leistungsfähigkeit unserer Gesellschaft, sondern auch für die zivile Sicherheit. Kaskadeneffekte, die sich aus der Störung eines Energieversorgungsnetzes ergeben, könnten verheerende Auswirkungen haben. Somit müssen

[27] Häring/Dörr 2005.





Schutzmaßnahmen entwickelt werden, die einerseits direkt auf die Widerstandsfähigkeit kritischer Infrastrukturen zielen und andererseits auch interdependente Infrastrukturen und Systeme vor schädlichen Effekten bewahren. Eine Ausschreibung sowohl zur Entwicklung von Beurteilungs- und Identifikationsmethoden zur Verwundbarkeit von Kraftwerken und Energieversorgungsnetzen als auch zur Verstärkung solcher Infrastruktureinrichtungen wird für das dritte Arbeitsprogramm zum Thema Sicherheit des 7. Forschungsrahmenprogramms[28] erwartet.

1.3.1.4 INFORMATIONSTECHNOLOGIEN UND BIOMETRIE

Informations- und Kommunikationstechnologien (IKT) haben in vielen Produktions- und Dienstleistungsbereichen eine zentrale Stellung in unserer heutigen Informations- und Wissensgesellschaft. Die Sicherheit von Computersystemen und Netzwerken ist daher auch für die Sicherheit der gesamten Bevölkerung von großer Bedeutung. Vor diesem Hintergrund verwundert es zunächst, dass gegenwärtig nur wenige Sicherheitsforschungsprojekte in den Themenfeldern „Information Systems" und „Computing Technologies" aktiv sind (vgl. Abbildung 3). Erklären lässt sich dies dadurch, dass Entwicklungen im Bereich IKT sowohl auf europäischer als auch auf nationaler Ebene in Parallelprogrammen gefördert werden.[29] Aspekte zur Sicherheit von IKT (zum Beispiel Internet, Datentransfer und -verwaltung, Kontrollsysteme, Software) gegenüber kriminellen Angriffen oder Missbrauch stellen dabei ein zentrales Anliegen dar. Innovative Verschlüsselungstechnologien zur sicheren Datenübertragung und sich selbst überprüfende und anpassende Netzwerke sind nur einige Beispiele für aktuelle Entwicklungen in der IT-Sicherheit. Widerstandsfähige Netzwerke mit einem zuverlässigen Sicherheitsmanagement sind auch Grundlage für die sichere Funktion kritischer Infrastrukturen (unter anderem Versorgungs- und Transportsysteme) und beispielsweise unverzichtbar im Bereich des Krisenmanagements und der Koordination von Einsatzkräften. Einige Projekte, die im Rahmen des IKT-Forschungsbereichs des 7. Forschungsrahmenprogramms derzeit durchgeführt werden, zielen auch auf Technologien, die direkt für die zivile Sicherheit eingesetzt werden können. Beispielsweise gehören hierzu die Entwicklung eines Terahertz-Verstärkers, die Widerstandsfähigkeit von Funksensornetzen oder ad-hoc Personal Area Networks (PAN) und Entwicklungsaspekte von Drohnen und Unterwasservehikeln zur Sicherheitsüberwachung von Objekten. Diese Beispiele zeigen, dass es deutliche Überlappungen zwischen den Forschungsbereichen IKT und Security gibt. Das BMBF hat daher für die IT-Sicherheitsforschung in den nächsten fünf Jahren Fördermittel in Höhe von 30 Mio. Euro vorgesehen.[30] Darüber hinaus untersucht das Bundesamt für Sicherheit in der Informationstechnik (BSI) als zentraler IT-Sicherheitsdienstleister des




---

[28] Die Ausschreibung ist für den Juli 2009 vorgesehen.

[29] Nationales Forschungsförderungsprogramm: IKT 2020 – Forschung für Innovationen (Laufzeit 2007 bis 2011).

[30] BMBF 2009c.





Bundes mögliche Risiken und Gefahren beim Einsatz von Informationstechnik, entwickelt entsprechende Sicherheitsvorkehrungen und analysiert Entwicklungen und Trends in der Informationstechnik.

Ebenfalls im Forschungsbereich IKT des europäischen Rahmenprogramms werden derzeit Projekte zum Thema Biometrie gefördert. Entwicklungsansätze sind hierbei beispielsweise die multiple biometrische Authentifizierung von Personen oder die Kombination von Kryptografie und Fingerbiometrie, um eine äußerst zuverlässige biometrische Identifikation zu erreichen bei gleichzeitiger Gewähr von Datenschutz und Privatsphäre. Eine Ausschreibung im Bereich Biometrie innerhalb des deutschen Sicherheitsforschungsprogramms ist noch nicht erfolgt, was die geringe Forschungsaktivität zu diesen Themen erklärt (vgl. Abbildung 3). Weitere technologische Innovationen sind hier also noch zu erwarten.

1.3.2 MÄRKTE FÜR SICHERHEITSTECHNOLOGIEN

Sicherheitstechnologien dienen nicht nur der Erhöhung der Sicherheit, sie haben auch ein großes wirtschaftliches Potenzial. Der Markt für sicherheitstechnische Produkte und Dienstleistungen hatte 2005 allein in Deutschland ein Umsatzvolumen von 10 Mrd. Euro bei hoher Wachstumsrate. Eine Förderung ziviler Sicherheitstechniken bedeutet daher gleichzeitig eine große Chance für Zukunftsmärkte.[31]

Der Markt für Sicherheitstechnologien und -dienstleistungen ist sehr breit gefächert und umfasst ein Spektrum, das von Überwachungssystemen über biometrische Zugangskontrollen bis hin zu Maßnahmen zur baulichen Verstärkung von Gebäuden reicht. Die prognostizierten Wachstumsraten für verschiedene Sicherheitstechnologien weisen darauf hin, welche Technologien sich auf dem Markt von morgen wahrscheinlich durchsetzen werden. Auf der Grundlage verschiedener Marktstudien können hier nur beispielhaft einige vielversprechende Technologiefelder genannt werden.

Sensorik als Technologie mit einem weiten Anwendungsfeld wird unter anderem in der Flughafensicherheit (Gesamtwachstumsrate von 34,3 Prozent von 2005 bis 2010) und Containersicherheit eingesetzt. Forschung an Technologien zur echtzeitnahen Lokalisierung (RTLS) und automatischen Identifizierung von Gegenständen findet derzeit nur in moderatem Maße statt und zielt unter anderem auf die Integration von RFID-Sensoren in komplexe Systeme. Dem europäischen Markt für RFID-Systeme im Bereich der Containersicherheit wird beispielsweise eine Wachstumsrate von 7,7 Prozent, gemittelt für den Zeitraum 2006 bis 2013, vorausgesagt.[32]

---

[31] BMBF 2006.
[32] Frost/Sullivan 2007a.







Unabhängig von der Einsatzumgebung werden tragbare Gefahrstoff-Detektoren in den kommenden Jahren von steigender Bedeutung sein. Sensortechnologien zur berührungslosen Detektion von CBRNE[33]-Stoffen, zum Beispiel für das Explosivstoff-Screening unbeaufsichtigter Gepäckstücke an öffentlichen Orten, haben hohe Wachstumsaussichten am Markt.[34] Für Explosivstoff-Detektionssysteme an Flughäfen etwa wurde in einer Studie von 2007 eine Wachstumsrate von 52,5 Prozent prognostiziert (im Zeitraum von 2005 bis 2010).[35] Das zeigt, dass Markt und Forschung hier in die gleiche Richtung zielen.

Smart Cards, obwohl in der Forschung nicht mehr stark vertreten, haben dennoch ein globales Marktwachstum von 12 Prozent (von 2007 bis 2012).[36] Innerhalb der Sicherheitstechnologien werden Smart Cards vor allem im Bereich der Zugangskontrollen, insbesondere in Verbindung mit biometrischen Sensoren, eingesetzt. Letzere werden sich in Zukunft immer mehr durchsetzen. Derzeit wird zwar ein Großteil des Markts (44,5 Prozent) für biometrische Technologien immer noch von Regierungsanwendungen bestimmt;[37] Fingerabdruckscanner beispielsweise sind jedoch schon zur Massenware geworden. Auf dem europäischen Markt wird ein starkes Wachstum von über 60 Prozent für biometrische Sensortechnologien erwartet.[38]



Im Forschungsfeld der Videoüberwachung sind bereits viele Technologien verfügbar, die sich in einigen Bereichen fest in der Sicherheitsarchitektur etabliert haben. Der Markt für Videoüberwachungstechnologien (einschließlich CCTV) ist bereits relativ gesättigt. Dennoch wird für die nächsten Jahre von einem geringen Wachstum von 4,6 Prozent (von 2006 bis 2012) ausgegangen.[39] Ein Grund dafür ist die Entwicklung und zunehmende Umrüstung von einfachen, analogen Anlagen hin zu komplexen, vernetzten computergestützten Systemen. Aktuelle Forschungsthemen in diesem Bereich sind unter anderem die optische Detektion und das Tracking von Personen, Fahrzeugen oder Gepäckstücken, intelligente Bewegungsanalysen, die auffälliges Verhalten erkennen, sowie die Kombination der Signale von festinstallierten und tragbaren Überwachungskameras.

Da Faktoren wie Qualität und Zuverlässigkeit gerade auf dem Markt für Sicherheitstechnologien eine wichtige Rolle für den Erfolg eines Produkts spielen, stellt die Entwicklung international einheitlicher Standards eine besondere Herausforderung für die Zukunft dar.

33 Chemical, Biological, Radioactive, Nuclear, Explosives (CBRNE).
34 Frost/Sullivan 2005.
35 Frost/Sullivan 2007b.
36 Frost/Sullivan 2008a.
37 Frost/Sullivan 2009.
38 Frost/Sullivan 2008b.
39 Frost/Sullivan 2007c.







1.4 FAZIT UND AUSBLICK

Die zunehmende Konzentration der Bevölkerung in Ballungszentren, die verschiedenen, immer komplexer miteinander verwobenen Lebensbereiche und -funktionen sowie der Übergang zu einer global vernetzten Informations- und Dienstleistungsgesellschaft machen uns in vielfältiger Weise verwundbar für Angriffe, Naturkatastrophen und Störungen unterschiedlichster Art. In der Sicherheitsforschung geht es zentral um die Entwicklung einer sicheren, resilienten Infrastruktur und die Fähigkeit, Bedrohungen und Gefahren abzuwehren oder zu minimieren bzw. Krisen zu bewältigen. Sicherheit ist daher eng verknüpft mit anderen Schlüsselthemen wie Energie, Gesundheit, Mobilität und Kommunikation. Dabei stellt die Sicherheitsforschung ein wissenschaftliches und politisches Querschnittsthema dar, in dem unterschiedliche Disziplinen der Natur- und Geisteswissenschaften eng zusammenarbeiten müssen, um den sich verändernden Herausforderungen der zivilen Sicherheit gerecht zu werden. Im europäischen und deutschen Sicherheitsforschungsprogramm wird vor allem ein fähigkeits- bzw. szenarienorientierter Ansatz gewählt. Dies soll zur Entwicklung von systematischen, sicherheitsrelevanten Gesamtkonzepten führen, die, basierend auf Risikoanalysen, dazu beitragen, die Angreifbarkeit und Verwundbarkeit zu minimieren.




Die Sicherheitsforschung ist ein technologisches Querschnittsthema und umfasst ein sehr breites Spektrum an Technologien und Forschungsgebieten. Viele der Technologiefelder, die von Experten der Europäischen Union als entscheidend für eine zukünftige Gewährleistung der Sicherheit benannt werden, wurden in europäischen und nationalen Forschungsprogrammen bereits adressiert (siehe zum Beispiel Sensortechnologien). Zukunftsweisende Entwicklungen und vielversprechende Sicherheitslösungen sind aber auch in vielen anderen Themenfeldern zu erwarten, die in den Forschungsprogrammen bislang noch nicht so stark berücksichtigt worden sind. Es ist von entscheidender Bedeutung, dass die Sicherheitsforschung ebenso intensiv auch an diese prioritäre Forschungsfelder herangeht, um das gesamte Spektrum der benötigten Entwicklungen abdecken zu können. Hier müssen die Forschungsprogramme durch entsprechende Ausschreibungen nachsteuern und Themenbereiche vorantreiben, die in der aktuellen Forschung unterrepräsentiert sind.

Eine moderne Industrie- und Dienstleistungsgesellschaft kann nur dann sicher in die Zukunft investieren, wenn sie auf einer sicheren Infrastruktur aufbaut und den Menschen dabei die Freiheit bietet, diese zu nutzen. Durch die Entwicklung von ganzheitlichen Maßnahmen zum Schutz gegen terroristische Angriffe oder natürliche Ex-





tremereignisse können der Schutz kritischer Infrastrukturen entscheidend erhöht und Kaskadeneffekte vermieden werden. Eine sichere Energieversorgung wird in Zukunft eine Schlüsselrolle einnehmen. Sowohl die Informations- und Kommunikationssicherheit kritischer Energieinfrastrukturen als auch der bauliche Schutz zum Beispiel von Atomkraftwerken sind nicht nur wichtig für die wirtschaftliche Leistungsfähigkeit unserer Gesellschaft, sondern auch für die zivile Sicherheit. Daher müssen Schutzmaßnahmen entwickelt werden, die sowohl auf die Widerstandsfähigkeit kritischer Infrastrukturen direkt zielen als auch interdependente Infrastrukturen und Systeme vor schädlichen Effekten bewahren. Sollte doch etwas passieren, müssen die Einsatzkräfte hervorragend ausgebildet sein, sicher kommunizieren und selbst vor den Gefahren sicher sein, gegen die sie ankämpfen.

Sowohl der europäische als auch der deutsche Markt für Sicherheitstechnologien entwickeln sich derzeit noch. Um diese Marktpotenziale zu nutzen, ist es wichtig, jetzt die Entwicklung neuer, zukunftsweisender Technologien voranzutreiben. Zu beachten ist: Der Markt für viele wichtige Sicherheitstechnologien wird durch staatliche Beschaffungen und Bestimmungen getrieben, nicht durch rein wirtschaftliche Kriterien. Daher wird ein zentraler Punkt bei der Beeinflussung der Marktentwicklung die Frage der europäischen Standardisierung im Sicherheitsbereich sein, um kleinteilige nationale und regionale Lösungen zu vermeiden. Hier sollten Anreize geschaffen werden, dass sich auch deutsche Stakeholder an dem europäischen Prozess beteiligen.




Es gilt also, Sicherheitsforschung weiter zu stärken, wichtige Technologien und Fähigkeiten weiter zu fördern. Die Technologien der Zukunft sind dabei die, die unseren Lebensraum und unsere Infrastruktur gegen jede Art von Bedrohung absichern. Dazu gehören ebenso das Erkennen von Gefahren mittels Sensorik, das Unterbinden von Katastrophen beispielsweise durch einsturzsichere Bauten sowie die möglichst schnelle Rückkehr zur Normalität durch ein optimales Vorgehen der Rettungskräfte.

1.5 LITERATUR

ANR 2009
Agence Nationale de Recherche, ANR (Hrsg.): „Concepts Systemes et Outils pour la Securite Globale (CSOSG)". Paris, 2009.

Beyerer 2007
Beyerer, J.: „Preamble". In: Beyerer, J. (Hrsg.): Future Security. 2nd Security Research Conference. Karlsruhe, 2007.

Beyerer/Geisler 2007
Beyerer, J./Geisler, J.: „Verteidigungs- und Sicherheitsforschung". In: Strategie und Technik (2007), Nr. 2.





BMBF 2006
Bundesministerium für Bildung und Forschung, BMBF (Hrsg.): Die Hightech-Strategie für Deutschland. Berlin, 2006.

BMBF 2007
Bundesministerium für Bildung und Forschung, BMBF (Hrsg.): Forschung für die zivile Sicherheit – Programm der Bundesregierung. Berlin, 2007.

BMBF 2008
Bundesministerium für Bildung und Forschung, BMBF (Hrsg.): Forschung für die zivile Sicherheit – Detektion von Gefahrstoffen. Berlin, 2008.

BMBF 2009a
Bundesministerium für Bildung und Forschung, BMBF: Deutschland und Frankreich stärken Sicherheits-Forschung. (Pressemitteilung vom 30.1.2009.) URL: http://www.bmbf.de/press/2458.php [Stand: 22.7.2009].

BMBF 2009b
Bundesministerium für Bildung und Forschung, BMBF (Hrsg.): Forschung für die zivile Sicherheit – Schutzsysteme für Rettungs- und Sicherheitskräfte. Berlin, 2009.

BMBF 2009c
Bundesministerium für Bildung und Forschung, BMBF: Rachel: „Internet der Dinge bringt uns in die Zukunft“. (Pressemitteilung vom 03.3.2009.) URL: http://www.bmbf.de/press/2478.php [Stand: 15.3.2009].

Buller/Thoma 2006
Buller, U./Thoma, K.: Memorandum der Fraunhofer-Gesellschaft zur Sicherheitsforschung. München, 2006.

Committee on Science and Technology for Countering Terrorism 2002
Committee on Science and Technology for Countering Terrorism, National Research Council (Hrsg.): Making the Nation Safer: the Role of Science and Technology in Counter Terrorism. Washington D.C., 2002.

DHS 2008
Department of Homeland Security, DHS (Hrsg.): High-Priority Technology Needs. Washington D.C., 2008.





European Commission 2008
European Commission (Hrsg.): FP 7 Work Programme 2009, Cooperation, Theme 10: Security. Brüssel, 2008.

European Communities 2004
European Communities (Hrsg.): Research for a Secure Europe – Report of the Group of Personalities in the Field of Security Research. Brüssel, 2004.

European Communities 2006
European Communities (Hrsg.): Meeting the Challenge: the European Security Research Agenda – A Report from the European Security Research Advisory Board. Luxemburg, 2006.

Frost/Sullivan 2005
Frost/Sullivan (Hrsg.): European Homeland Security – A Market Opportunity Analysis. London, 2005.

Frost/Sullivan 2007a
Frost/Sullivan (Hrsg.): Container Security – A Market Analysis. London, 2007.



Frost/Sullivan 2007b
Frost/Sullivan (Hrsg.): European Airport Security Equipment Market: Investment Analysis. London, 2007.

Frost/Sullivan 2007c
Frost/Sullivan (Hrsg.): European CCTV and Video Surveillance Equipment Markets. London, 2007.

Frost/Sullivan 2008a
Frost/Sullivan (Hrsg.): World Smart Card Market. London, 2008.

Frost/Sullivan 2008b
Frost/Sullivan (Hrsg.): North American and Europe Biometrics Market – Investment Analysis. London, 2008.

Frost/Sullivan 2009
Frost/Sullivan (Hrsg.): Biometrics in Europe – Future Technologies and Applications. London, 2009.





Häring/Dörr 2005
Häring, I./Dörr, A.: "Risk Analysis Methodology for High Explosive Events". (Society for Risk Analysis Europe: Major Risks Challenging Publics, Scientists and Governments. Annual Conference 12.-14. September 2005.) Como, Italien, 2005 – Tagungsband.

Intelligence online 2008
Intelligence online: CSOSG, Breeding Ground for French Homeland Security. Newsletter Nr. 564, 14.-27. Februar 2008.

Reichenbach et al. 2008
Reichenbach, G./Göbel, R./Wolff, H./Stokar von Neuforn, S. (Hrsg.): Risiken und Herausforderungen für die öffentliche Sicherheit in Deutschland. (Grünbuch des Zukunftsforums öffentliche Sicherheit.) Berlin, 2008.

Riedel/Schäfer 2008
Riedel, W./Schäfer, F.: "Sensor Based Real-Time Situation Awareness of Critical Infrastructure". In: Thoma, Klaus (Hrsg.): Future Security (3rd Security Research Conference 2008; Fraunhofer Defense and Security Alliance). Stuttgart, 2008.




Thoma 2008
Thoma, K. (Hrsg.): Future Security. (3rd Security Research Conference 2008; Fraunhofer Defense and Security Alliance.) Stuttgart, 2008.





2 SICHERHEIT: SYSTEMANALYSE UND -DESIGN

JÜRGEN BEYERER/JÜRGEN GEISLER/ANNA DAHLEM/PETRA WINZER

2.1 EINLEITUNG

Ein technischer Prüfer untersucht die Achsen des ihm anvertrauten ICE sorgfältig auf Risse und bewahrt Bahnpassagiere damit vor einem möglicherweise katastrophalen Unfall. Mit demselben Ziel entwickelt ein Ingenieur einen Ermüdungswächter, der den Triebwagenführer des Zuges rechtzeitig vor dem Einschlafen warnt. Ein Mitarbeiter der „Airport Security" kontrolliert am Röntgenbildschirm aufmerksam das Bordgepäck von Fluggästen auf Waffen und Sprengstoff, um die Reisenden vor einem Terroranschlag zu schützen. Ein Versicherungsmakler nimmt einem Fabrikinhaber die Sorge vor dessen Ruin durch Hochwasser, indem er ihm eine Assekuranz gegen Elementarschäden verkauft.

Die vier Fälle stehen beispielhaft für vier wesentliche Kategorien von Gefährdungen: durch technisches und menschliches Versagen (ICE), durch feindselige Absicht (Flughafenkontrolle) und durch Naturereignisse (Hochwasserversicherung). Bahnpassagiere, Fluggäste und der Fabrikinhaber sind gewissermaßen Kunden von Dienstleistern wie dem Bahnprüfer, dem Entwicklungsingenieur, dem Gepäckkontrolleur oder dem Versicherungsvertreter. Jeder der Kunden würde wahrscheinlich ohne zu zögern bestätigen, dass dieses Dienstleistungsprodukt „Sicherheit" genannt wird. Allerdings würde er hierbei wahrscheinlich keinerlei Unterscheidung zwischen Safety und Security vornehmen.

Trotz der Gemeinsamkeit werden alle hier exemplarisch genannten Sicherheitsdienstleister die Prozesse, mit denen sie ihr jeweiliges Produkt erzeugen, wohl nicht nach demselben Leitfaden strukturieren. Zu unterschiedlich sind die Fälle auf den ersten Blick gelagert. Ist der Begriff „Sicherheit" also nur eine lose Sammelvokabel, welche ganz allgemein die Abwesenheit von Furcht vor Gefahren beschreibt? Oder gibt es eine so starke Gemeinsamkeit zwischen ganz unterschiedlichen Sicherheitsfällen, dass es gerechtfertigt ist, sie unter ein gemeinsames Theoriedach zu stellen? Kann der Systems-Engineering-Ansatz[1] für die Entwicklung dieses Theoriedachs genutzt werden? Wäre ein solches

[1] Hollnagel et al. 2006; Sitte/Winzer 2004.





Dach nützlich für die Analyse von Gefährdungen in und außerhalb von verschiedensten Systemen bzw. deren Systemelementen? Können darauf aufbauend Gefährdungs- und/ oder Sicherheitsprognosen mittels Modellbildung und Simulation systematischer erstellt werden? Wäre es nützlich für die Entwicklung von Sicherheitskonzepten (Minimierung bzw. Beseitigung von ungewollten und gewollten Gefahren), einen allgemeinen Systemansatz zu entwickeln, um so einen theoriegestützten Beitrag für die Entwicklung der Brücke zwischen Safety und Security zu erarbeiten?[2]

In einer ungebremst komplexer werdenden Gesellschaft mit immer weniger zu überschauenden und räumlich entgrenzten persönlichen und technischen Wechselbeziehungen sowie einer immer höheren Abhängigkeit von technischer Infrastruktur wird Sicherheit zu einem besonders wertvollen, aber auch besonders schwierig zu „fertigenden" Produkt. Könnte ein nichttriviales generisches Kernmodell für Systeme gefunden werden, in denen Sicherheit eine wesentliche Rolle spielt und mit denen Sicherheit gewährleistet wird, so wäre dies ein wesentlicher Beitrag, um inmitten der vielen Bäume der einzelnen Sicherheitsprobleme und -lösungen den Wald zu sehen und damit das Produkt „Sicherheit" in Zukunft effektiver und effizienter herstellen und anbieten zu können.[3] Nachfolgend wird in Abschnitt 2.2 zunächst dieses Produktsystem genauer betrachtet. Nach einem ersten Fazit in Abschnitt 2.3 erfolgt darauf aufbauend in Abschnitt 2.4 die Ableitung eines theoretischen Daches unter Nutzung des Systems-Engineering-Ansatzes. Abschnitt 2.5 fasst die Ideen und zu lösenden Forschungsfragen in diesem Kontext zusammen.



2.2 DAS PRODUKTSYSTEM „SICHERHEIT"

In den oben genannten Beispielfällen spielen immer drei trennbare Entitäten eine Rolle, die miteinander wechselwirken und so ein System bilden: Der Schutzbedürftige (ICE-Fahrgast, Fluggast, Versicherungskunde), der Gefährder (Ermüdungsriss in der ICE-Achse, übermüdeter Triebwagenführer, Terrorist, Hochwasserwelle)[4] und der Schützer (technischer Prüfer, Entwicklungsingenieur, Versicherungsgesellschaft). Abbildung 1 zeigt diese Entitäten als Basiselemente des Systems „Sicherheit", zunächst noch ohne näher benannte Wechselbeziehungen.

---

2 Die VDI-Denkschrift „Qualitätsmerkmal ‚Technische Sicherheit'" (DIN 2005) konzentriert sich auf den Safety-Aspekt des deutschen Begriffs „Sicherheit". In diesem Beitrag werden hingegen insbesondere der Security-Aspekt und eine Vereinheitlichung beider Aspekte in einer übergreifenden Systematik betrachtet.

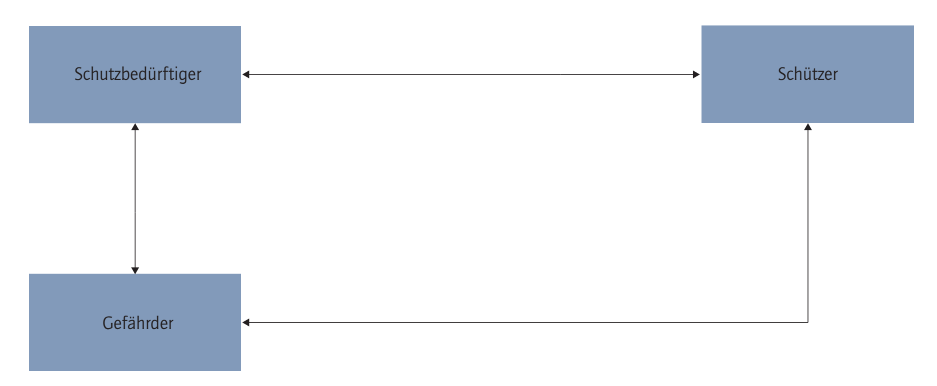
3 Beyerer 2009.

4 Der Begriff „Gefährder" umfasst hier auch sächliche Ursachen von Gefahren. Nach DIN 820-120 wird zwar eine potenzielle Schadensquelle als „Gefährdung" bezeichnet. Der Begriff „Gefährdung" steht aber im Grunde für einen Vorgang und nicht für ein Systemelement. Deshalb soll das potenziell gefährdende Systemelement hier immer als „Gefährder" bezeichnet werden.





Abbildung 1: Die Basiselemente des Systems „Sicherheit“






Die Elemente des Systems sind unterschiedliche Rollen und nicht zwingend getrennte physische Entitäten. So kann ein Mensch, der sich selbst schützt, Schutzbedürftiger und Schützer zugleich sein. Desgleichen besteht auch die Möglichkeit, dass sich ein Mensch selbst gefährdet. Dann fallen die Rollen Schutzbedürftiger und Gefährder in einer physischen Entität zusammen. Selbst die Rollen von Schützer und Gefährder können in einer Entität zusammenfallen. Sollte die Systemanalyse allerdings eine solche Konstellation ergeben, muss sie dringend aufgelöst werden, da diese beiden Rollen Antagonisten sind.

Das Element „Schützer“ soll so gestaltet werden, dass es seine Schutzaufgabe möglichst gut erfüllt und damit ein hohes Maß an Sicherheit gewährt. Es ist das Ziel des System-, das heißt des Teilsystementwurfs. Voraussetzung dafür ist, dass die Schnittstellen des schützenden Systems zu seiner Umgebung bezogen auf die Schutzaufgabe bekannt sind. Ohne diese Schnittstellen hinge das schützende System gewissermaßen „in der Luft“ und der technische/organisatorische Entwurf würde nicht gelingen. Ziel der Ausführungen in diesem Abschnitt ist es, Grundlagen für die Bestimmung dieser Schnittstellen zu legen.





Nach der Definition der Elemente ist der nächste wesentliche Schritt der Systemanalyse, die Wechselbeziehungen zwischen den Elementen zu bestimmen. Im Folgenden sollen die Wechselbeziehungen aus Abbildung 1 der Reihe nach analysiert werden. Die Analyse beginnt mit der für ein Sicherheitsproblem ausschlaggebenden Wechselbeziehung zwischen dem Schutzbedürftigen und dem Gefährder.

2.2.1 WECHSELBEZIEHUNG VON SCHUTZBEDÜRFTIGEM UND GEFÄHRDER

Bestimmend für den Schutzbedürftigen ist seine Verwundbarkeit. Wir definieren „Verwundbarkeit" wie folgt:

> *Verwundbarkeit ist die Eigenschaft des Schutzbedürftigen, für Ereignisse empfänglich zu sein, die ihn in unerwünschte Zustände führen*.

Wir konzentrieren uns hier ausschließlich auf Ereignisse, die von außen kommend auf den Schutzbedürftigen einwirken.[5] So ist die Verwundbarkeit also genauer betrachtet eine Eigenschaft der Hülle des Schutzbedürftigen. Gegenüber dem Gefährder sprechen wir von Flanken der Verwundbarkeit. Diese kennzeichnen verschiedene Qualitäten der Empfänglichkeit des Schutzbedürftigen. Betrachtet man, was nahe liegt, als Erstes die körperliche Hülle des Menschen als Schutzbedürftigem, so kann ihm beispielsweise eine mechanische Verwundbarkeitsflanke zugeordnet werden, die seine Empfindlichkeit gegenüber Schadeinwirkungen wie Schlägen, Stößen, Stichen oder Schnitten bestimmt. Eine biochemische Flanke lässt sich mit Bezug auf Gifte, Krankheitskeime und Ähnliches, eine radiologische mit Bezug auf Schadeinwirkungen durch Strahlung usw. definieren. Ebenso ist eine informatorische Flanke der Verwundbarkeit vorstellbar, über welche Nachrichten an den schutzbedürftigen Menschen herangetragen werden, die ihm beispielsweise seelischen Schaden zufügen.




Die körperliche Hülle des schutzbedürftigen Menschen ist jedoch nicht die einzige Projektionsfläche für seine Flanken der Verwundbarkeit. Die mit dem Begriff „Schutzbedürftiger" bezeichnete Entität muss zwar mindestens einen Menschen enthalten, kann jedoch auch selbst wiederum ein System von Menschen und Sachen sein. Wenn also beispielsweise Menschen untereinander kommunizieren wollen und diese Kommunikation gestört wird, beispielsweise durch Schadeinwirkungen auf das Fernsprechnetz, dann liegt die Flanke der Verwundbarkeit aufseiten dieser technischen Infrastruktur, obwohl der eigentliche Schaden bei den beteiligten Menschen entsteht.

---

[5] Innere Eigenschaften des Schutzbedürftigen, die, ohne dass jemals eine Einwirkung von außen stattgefunden hat, zu einem unerwünschten Zustand führen, wie beispielsweise eine Erbkrankheit, bleiben hier außer Betracht. Ihre Betrachtung würde das Basismodell aus Abbildung 1, das eine äußere Gefährdung voraussetzt, überdehnen.





Der Gefährder wirkt auf die Flanken der Verwundbarkeit des Schutzbedürftigen und wir können auf dieser Grundlage feststellen:

> *Gefährder ist jedes Objekt im Umfeld des Schutzbedürftigen, das in nennenswertem Umfang auf dessen Flanken der Verwundbarkeit wirken kann.*[6]

Ziel unserer Betrachtung ist es, Maßnahmen ableiten zu können, welche die Sicherheit des Schutzbedürftigen erhöhen. Eine naheliegende Maßnahme ist die Härtung der verwundbaren Flanken. Sie kann beispielsweise dadurch geschehen, dass dem Schutzbedürftigen zum Tragen eines Helmes geraten wird, um seine mechanische Flanke zu härten (Beispiel für eine äußere Härtung), oder ihm eine Schutzimpfung empfohlen wird, um ihn biochemisch weniger empfindlich zu machen (Beispiel für eine innere Härtung). Die Maßnahme der Härtung von Flanken der Verwundbarkeit entfaltet sich am Schutzbedürftigen selbst. Welche Gegenwirkung kann der Schutzbedürftige auf den Gefährder selbst ausüben, um sich ein höheres Maß an Sicherheit zu verschaffen?

Zur klaren Rollentrennung soll hier eine direkte, willentliche Einwirkung des Schutzbedürftigen auf den Gefährder ausgeschlossen und diese vollständig auf die Rolle des Schützers übertragen werden. Diese wird später in Abschnitt 2.2.3 („Die Leistung des Schützers“) erörtert. Dennoch gibt es eine Wirkung des Schutzbedürftigen in Richtung des Gefährders, um dessen Schadeinwirkung zu mindern: nämlich die, sich vom Gefährder fernzuhalten. Dafür wird zwischen dem Gefährder und dem Schutzbedürftigen die, stets passive, Entität des Übertragungswegs eingeführt. Der Übertragungsweg transportiert eine vom Gefährder ausgelöste Wirkung hin zum Schutzbedürftigen. Ist der Gefährder beispielsweise der Riss in der ICE-Achse, dann ist der Übertragungsweg die gesamte mechanische Kette von der Achse bis zum Sitz des Fahrgastes, also zu dem Punkt, an dem die Wirkung die Flanke der Verwundbarkeit trifft. Je weiter entfernt der Schutzbedürftige vom Gefährder ist, desto weniger wird ihn, jedenfalls in den meisten Fällen, die vom Gefährder ausgelöste Wirkung treffen. Abbildung 2 veranschaulicht diese Wirkungsbeziehung.

Sich vom Gefährder fernzuhalten, ist eine Handlung, die der Schutzbedürftige selbst ausführen muss, zu die ihm aber der Schützer – und darin besteht möglicherweise ein Teil seiner Leistung – raten kann.

---

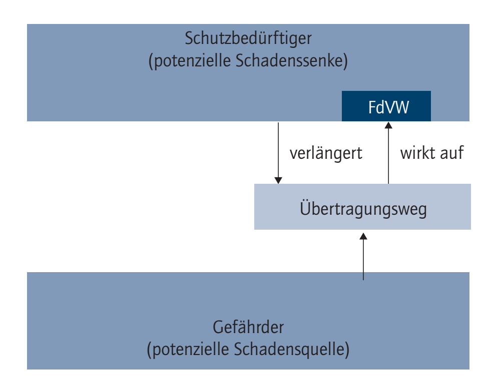
6 Auch Menschen als Verursacher einer Gefährdung werden, aus der subjektiven Sicht des Schutzbedürftigen, als „Objekt“ bezeichnet.







Abbildung 2: Wechselbeziehung zwischen dem Gefährder als potenzielle Schadensquelle und dem Schutzbedürftigen als potenzielle Schadenssenke mittels des Übertragungswegs



FdVw: Flanken der Verwundbarkeit



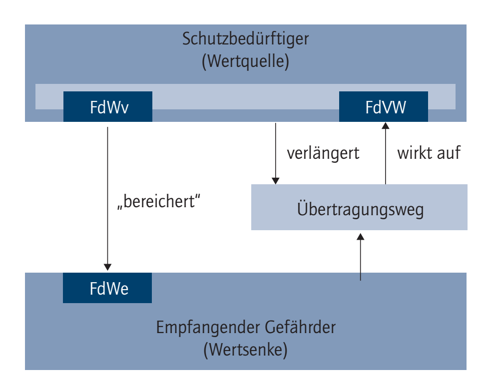


Der Ausschluss der direkten Wirkung aus der Rolle des Schutzbedürftigen auf den Gefährder gilt allerdings nur für Einwirkungen, die mit der Absicht vorgenommen werden, den Gefährder daran zu hindern, eine Schadwirkung zu entfalten. Vergegenwärtigen wir uns aber als Beispiel die Gefährdung des Schutzbedürftigen durch einen Räuber, dann erhält dieser bei erfolgreicher Schadandrohung oder -einwirkung einen Gegenwert für seine „Bemühung", nämlich die Beute. Diese wird ihm vom Schutzbedürftigen nicht freiwillig gegeben. De facto aber fließt sie von diesem zum Gefährder hin. Am Beispiel des Räubers orientiert kann man sagen, dass der Schutzbedürftige den Gefährder bereichert. Er empfängt etwas von dem Schutzbedürftigen, der aus Sicht des empfangenden Gefährders eine Wertquelle darstellt, während jener zur Wertsenke wird. Für diesen Fall muss also die Darstellung von Abbildung 2 zu der Darstellung in Abbildung 3 ergänzt werden. Darin werden auch zwei zusätzliche Klassen von Flanken eingeführt: die Flanken der Wertveräußerung (FdWv) auf der Seite des Schutzbedürftigen und die Flanken des Wertempfangs (FdWe) aufseiten des Gefährders. Die FdWv und die FdWe beim Schutzbedürftigen sind in Abbildung 3 (siehe unten) mit einem gemeinsamen Rahmen unterlegt. Dies zeigt an, dass beide Flanken zusammenfallen können, zum Beispiel im Falle eines Diebstahls. Dort wird die materielle „Verwundung" durch gegenleistungslosen Entzug von Werten zugefügt, ohne dass ein leiblicher Schaden zugefügt wird. Demgegenüber ist der Raub in der Regel mit einem Akt körperlicher Gewalt verbunden, der aber nur als Mittel dient, um einen Wertfluss vom Schutzbedürftigen zum Gefährder einzuleiten.





Abbildung 3: Wechselbeziehung zwischen Schutzbedürftigem und empfangendem Gefährder



FdWv: Flanken der Wertveräußerung
FdWe: Flanken des Wertempfangs

Dieser Wertfluss vom Schutzbedürftigen hin zum Gefährder markiert den fundamentalen Unterschied zweier Gefährdungskategorien: der gewollten und der ungewollten Gefährdung.




- *Gewollte Gefährdung liegt vor, wenn der Gefährder durch die Schadeinwirkung auf die Schadenssenke von dieser einen gewollten Wertzuwachs erfährt.*
- *Ungewollte Gefährdung dagegen liegt vor, wenn der Gefährder durch die Schadeinwirkung auf die Schadenssenke von dieser keinen gewollten Wertzuwachs erfährt.*

2.2.1.1 GEWOLLTE GEFÄHRDUNG

Der vom Gefährder intendierte Wertzuwachs kann materieller Natur sein, wie zum Beispiel bei dem oben erwähnten Dieb oder Räuber. Er kann aber auch ideeller Natur sein, wie beispielsweise wenn ein um Selbstachtung ringender junger Mensch seine Mitschüler tötet, um – wenigstens für kurze Zeit – einen Wertzuwachs seiner Persönlichkeit zu empfinden. Diese beiden Beispiele markieren auch zwei Pole der gewollten Gefährdung. Im Fall des materiellen Wertzuwachses wird der Räuber als Gefährder und Wertsenke die Höhe der Schadeinwirkung auf den Schutzbedürftigen als Wertquelle nach den Kosten des dazu nötigen Eigenaufwands kalkulieren. Der Räuber wählt die Schadeinwirkung auf die Wertquelle bzw. deren Androhung als Alternative zum Angebot einer Gegenleistung an den Schutzbedürftigen. Er ist nicht am Leiden der Wertquelle interessiert,





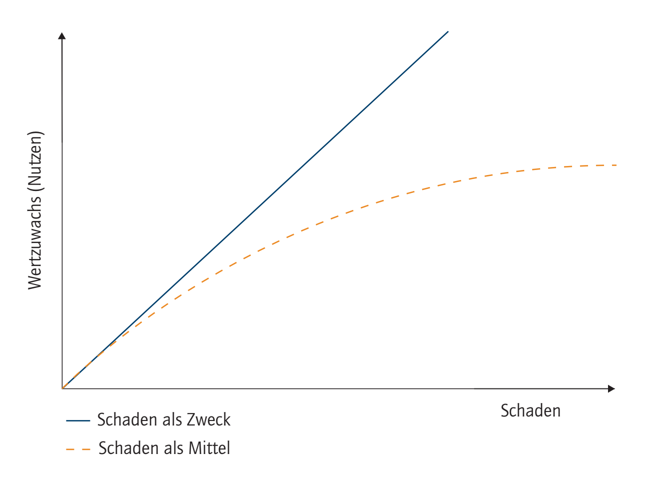
sondern nutzt diese nur als einen, nach seiner Kalkulation aufwandssparenden Hebel, um vom Schutzbedürftigen eine Leistung zu erhalten. Ein an materiellem Wertzuwachs interessierter Gefährder orientiert sich also bei seiner Schadeinwirkung am Minimalprinzip und fügt dem Schutzbedürftigen nicht mehr Schaden zu als nötig ist, um an den gewünschten Wert zu gelangen.

Dagegen ist der Amokschütze, wie auch ein Selbstmordattentäter, an der Maximierung des Schadens beim Schutzbedürftigen interessiert, weil er aus diesem seinen Wertzuwachs schöpft. Gefährder dieser Kategorie gehen nach dem Maximalprinzip vor.

Wir erkennen also innerhalb der Klasse der gewollten Gefährdungen zwei Klassen von Gefährdern: die Gefährder, die den Schaden am Schutzbedürftigen als Mittel betrachten (Beispiel Räuber) und diejenigen, die ihn als Zweck sehen (Terrorist, Amokschütze). Im Falle des Schadens als Zweck steigt der Wertzuwachs linear mit dem angerichteten Schaden. Im Fall des Schadens als Mittel verlangsamt sich der Wertzuwachs eher mit höher werdendem Schaden. Denn es ist anzunehmen, dass ab einer gewissen Schadenshöhe eine Wirkungssättigung beim Schutzbedürftigen als Wertquelle eintritt und er keinen schadensproportionalen Zuwachs an Wert für den Gefährder mehr bereithält. Abbildung 4 veranschaulicht qualitativ diese angenommene Beziehung.




Abbildung 4: Qualitative Beziehung zwischen dem vom Schutzbedürftigen erlittenen Schaden und dem von einem empfangenden Gefährder erreichten Nutzen in Form von Wertzuwachs



Der an materiellem Nutzen interessierte Gefährder bemisst die Höhe seines Schädigungs- bzw. Schädigungsdrohungsaufwands nach dem erwünschten Wertzuwachs. Davon ausgehend, dass der beim Schutzbedürftigen erzielte Schaden auch nicht linear mit

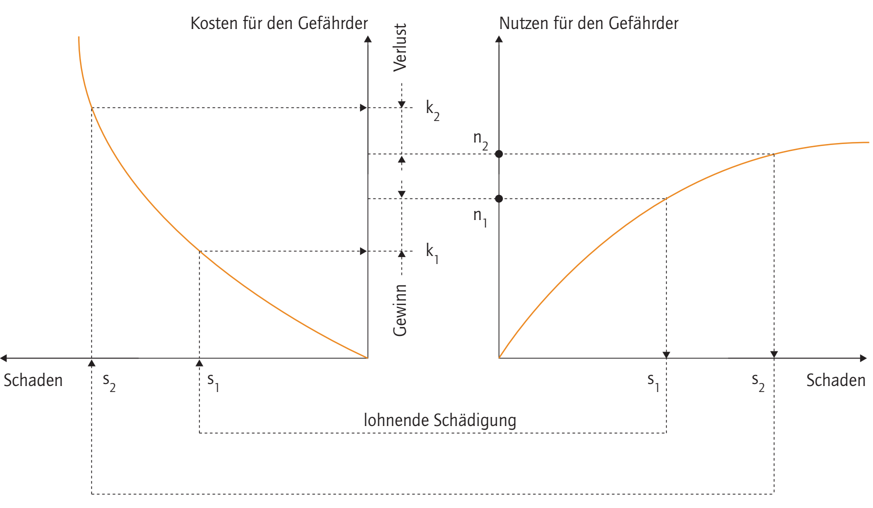




dem Schädigungsaufwand steigt, sondern sich einem Grenzwert nähert, und mithilfe der Annahme, dass der Gefährder eine Vorstellung von diesen Abhängigkeiten besitzt, kann er sich ausrechnen, welche Kosten-/ Nutzenrelation für ihn lohnend ist. Schädigungsaufwand (Kosten) und Wertzuwachs durch den Schutzbedürftigen (Nutzen) werden in derselben Währung gehandelt. Abbildung 5 veranschaulicht diese Überlegung des materiell interessierten Gefährders. Ausgehend von einem intendierten Nutzen schätzt er die Höhe des Schadens s ab, den er der Wertquelle androhen oder auf diese ausüben muss, um n zu erzielen (rechtes Teildiagramm). Mit dem erforderlichen Schaden s geht er dann in die Schaden/Kosten-Beziehung (linkes Teildiagramm), liest dort seine Kosten k für die Schädigungsaufwendungen ab und kann sich ausrechnen, ob die Differenz von k und n für ihn lohnend ist.




Abbildung 5: Ermittlung der Kosten-/ Nutzenrelation bei Schädigung als Mittel zum Zweck materiellen Wertzuwachses



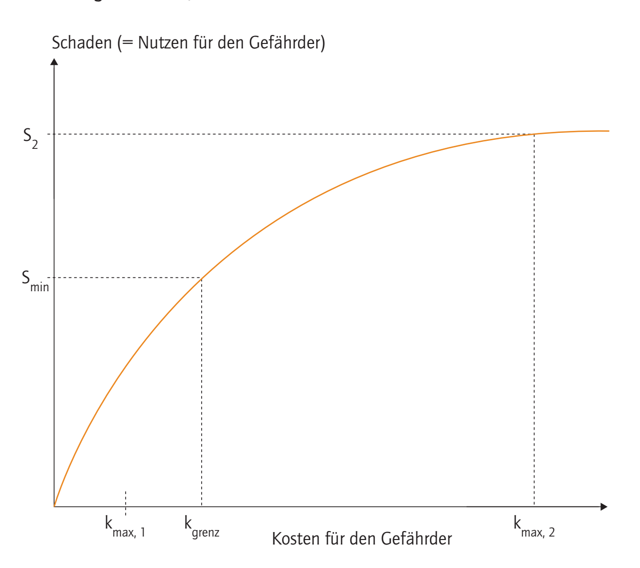
Für den Gefährder, der den Schaden als Zweck betrachtet, ist eine solche Rechnung nicht sinnvoll. Kosten für die Schädigung und deren Nutzen werden nicht in der gleichen Währung abgerechnet. Ein solcher Gefährder setzt sich vielmehr ein minimales Schädigungsziel und überlegt sich, ob er mit dem maximalen Aufwand, den er zu betreiben in der Lage ist, diesen Minimalschaden erzielen kann. Wenn ja, dann übt er die Schadwirkung mit maximalem Aufwand aus, ungeachtet dessen, ob er sich damit schon in einem ungünstigen Bereich der Aufwands-/ Schadensfunktion befindet. Wenn





nein, unterlässt er die Schädigung. Dies wird mit Abbildung 6 veranschaulicht. Der minimal vom Gefährder gewollte Schaden s_{min} ist zu den Kosten k_{grenz} zu erzielen. Kann der Gefährder nur maximal Kosten in Höhe von $k_{max,1} < k_{grenz}$ aufbringen, dann wird er keinen Schaden ausüben. Sind die maximal für ihn erträglichen Kosten $k_{max,2} > k_{grenz}$, dann wird er diese Kosten aufbringen, um den Schaden zu erzielen, ungeachtet der Tatsache, dass er entsprechend diesem Diagramm zu nennenswert geringeren Kosten beinahe den gleichen Schaden erzielen könnte.

Abbildung 6: Kosten-/ Nutzenkalkulation im Fall des Schadens als Zweck






Die beiden Kategorien „Schaden als Mittel“ und „Schaden als Zweck“ sind, wie oben bereits erwähnt, nur zwei Pole, zwischen denen sich Mischformen realer Gefährdungen entfalten. So ist vielen Menschen, die eine Schädigung anderer als Mittel einsetzen, eine gewisse Lust an der Gewaltausübung zu eigen, die sie über das für ihre materiellen Interessen notwendige Maß an Gewalt hinausschießen lässt. Andererseits sind viele Selbstmordattentäter zwar selbst zum Preis ihres eigenen Lebens an möglichst hohem Schaden interessiert. Sind sie aber im Auftrag einer Terrororganisation unterwegs, werden ihre Entsender, die ja ihre Leben selbst nicht aufs Spiel setzen, die Kosten und Nutzen durchaus kühl kalkulieren. Das Gefährderteilsystem Terrororganisation handelt also nach anderen Maximen als dessen Element Selbstmordattentäter.





Unabhängig davon, ob die Schädigung als Mittel oder als Zweck ausgeübt wird, sucht sich der wollende Gefährder stets die schwächste Flanke der Verwundbarkeit. An ihr kann derjenige, der den Schaden als Mittel betrachtet, mit geringstem Aufwand den aus seiner Sicht nötigen Schaden ausüben oder androhen. Derjenige, der den Schaden als Zweck will, kann mit dem von ihm angesetzten Aufwand den höchsten Schaden bewirken. Im Falle gewollter Gefährdung bestimmt also die schwächste Flanke die Verwundbarkeit.

2.2.1.2 UNGEWOLLTE GEFÄHRDUNG

Gewollte Gefährdung kann nur durch willensbegabte Wesen erfolgen. Wir beschränken uns hier auf Menschen als willensbegabte Wesen.[7] Ungewollte Gefährdung dagegen kann sowohl durch fahrlässiges Verhalten von Menschen als auch durch Naturprozesse ausgelöst werden, zum Beispiel Wetterphänomene oder Erdbeben. Im Fall der ungewollten Gefährdung ist der Wert-Fluss vom Schutzbedürftigen zum Gefährder irrelevant, wobei er nicht ausgeschlossen wird. Obwohl in beiden Fällen Zufallsprozesse am Werk sind, sollte die ungewollte Gefährdung durch Menschen von der durch die Natur unterschieden werden. Während wir nämlich Naturereignissen kein Kostenbewusstsein unterstellen, ist dies bei Menschen grundsätzlich anzunehmen. Fahrlässigkeit zu vermeiden aber verursacht Kosten. Der fahrlässige Gefährder erfährt einen indirekten Wertzuwachs dadurch, dass er durch Inkaufnahme der Schädigung eines Anderen eigene Aufwendungen spart.



Die entscheidende Differenzierung der menschlich fahrlässigen Gefährdung von der gewollten Gefährdung ist die, dass der wollende Gefährder, der seinen Wertzuwachs vom Geschädigten erwartet, Aufwand treibt, um Schaden auszuüben oder anzudrohen. Dahingegen wirkt der nicht wollende Gefährder gerade dadurch, dass er den Aufwand zur Schadensvermeidung spart, möglicherweise schädigend. Diese Beziehung kann in dem Wechselwirkungsschema entsprechend Abbildung 2 noch nicht ausgedrückt werden.

Unabhängig davon, ob die ungewollte Gefährdung durch fahrlässige Menschen oder Naturereignisse geschieht, ist die erreichte Flanke der Verwundbarkeit beim Schutzbedürftigen zufällig. Es gibt hier keine wie auch immer geartete Anziehungswirkung schwacher Verwundbarkeitsflanken auf den Gefährder. Gleichwohl leidet der Schutzbedürftige mehr, wenn zufällig eine seiner schwachen Flanken getroffen wird.

Abbildung 7 gibt einen Überblick über die genannten Kategorien der Gefährdung. Mangels griffiger deutscher Worte wird die Sicherheit vor gewollter Gefährdung oft als „Security", die vor ungewollter Gefährdung als „Safety" bezeichnet.

[7] Betrachtet man pathogene Mikroorganismen, die Resistenzen gegen pharmazeutische Wirksubstanzen entwickeln, so kann man dem evolutionären Prozess, der diese Anpassung bewirkt, ein quasi-intelligentes Verhalten zuschreiben, das in der hier aufgezeigten Systematik phänomenologisch wie eine gewollte Gefährdung zu behandeln wäre (Hinweis von K. Vieweg zu einer Entwurfsversion dieses Aufsatzes).







Abbildung 7: Taxonomie der Gefährdungskategorien

2.2.2 WECHSELBEZIEHUNG VON SCHUTZBEDÜRFTIGEM UND SCHÜTZER





Die Analyse des Systems Sicherheit geht vom Schutzbedürftigen aus und nimmt an, dass dieser als Kunde den Schützer beauftragt. Schutzbedürftiger und Schützer gehen also eine Dienstleistungsbeziehung ein. Deshalb kann man den Schutzbedürftigen auch als Sicherheitsdienstnehmer, den Schützer dagegen als Sicherheitsdienstgeber bezeichnen. Wir gehen davon aus, dass der Schutzbedürftige zwar in gewisser Weise schwach (sonst wäre er nicht des Schutzes bedürftig), aber in diesem Prozess der mündige Souverän ist. Dies drückt sich darin aus, dass er seinen Sicherheitsbedarf selbst bestimmt und diesen dem Schützer übermittelt.[8] Als Gegenleistung befriedigt der Schützer den Sicherheitsbedarf seines Kunden. Schutzbedürftiger und Schützer schließen gewissermaßen einen Schutzvertrag (siehe Abbildung 8).[9] Der Schutzvertrag ist hier abstrakt gemeint und erstreckt sich von dem (virtuellen) Vertrag einer Person mit sich selbst als Schützer (wenn beide Rollen in einer Person zusammenfallen) über private Verträge von natürlichen oder juristischen Personen mit privaten Sicherheitsdienstleistern bis zu der über den generellen Gesellschaftsvertrag geregelten Rolle des Staates als Schützer seiner als generell schutzbedürftig angenommenen Bürger.

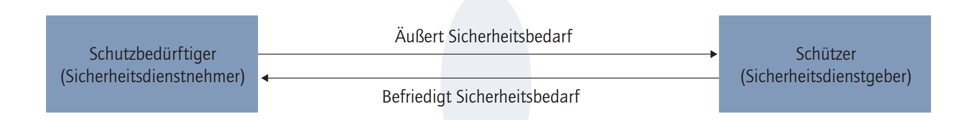
8 Nicht jeder mündige Bürger wird das in jedem Einzelfall tun, sondern sich durchaus gesellschaftlich gängigen Sicherheitsvorstellungen anpassen bzw. unterwerfen (siehe Gurtpflicht). Wir gehen aber von einer politischen Ordnung aus, innerhalb derer die Bürger Einfluss auf die gesellschaftlich gängigen Sicherheitsvorstellungen haben. So ist ja auch die Gurtpflicht in Deutschland Resultat eines demokratischen Prozesses.

9 Der Begriff „Vertrag" möge hier nicht im engeren juristischen Sinne gelten, sondern als Beschreibung einer allgemein oder für den Einzelfall willentlich eingegangenen Beziehung, die durch Leistung und Gegenleistung definiert ist.






Abbildung 8: Wechselbeziehung zwischen Schutzbedürftigem und Schützer



Ausschlaggebend für die Dienstleistungsbeziehung zwischen Schutzbedürftigem und Schützer ist ein klar bestimmter Sicherheitsbedarf. Die „Sicherheit“, umgangssprachlich als feste Überzeugung verstanden, dass ein bestimmtes Ereignis eintreten wird („ich bin mir sicher, dass morgen die Sonne wieder aufgehen wird“), hat im Kontext dieses Diskurses eine auf schädliche Ereignisse eingeschränkte Bedeutung. Ereignisse sind Ausdruck von Zustandsübergängen. So ist es letztlich der Übergang in einen für ihn schädlichen Zustand, den zu vermeiden der Schutzbedürftige vom Schützer erwartet. Schaden verursacht Kosten, die nach Eintritt des Schadens aufgewendet werden müssen, um diesen zu beheben.




Der Schutzbedürftige wird sich bei der Formulierung des Sicherheitsbedarfs gegenüber dem Schützer in aller Regel zunächst auf diejenigen Zustände beschränken, von denen er fürchtet, dass sie ihm Kosten verursachen, wohingegen er diejenigen Zustände, die er zu erreichen beabsichtigt, die ihm also Nutzen bringen, im Kontext des Sicherheitsbedarfs oft ausblendet. Diese sind aber wesentlich, weil ihre Vernachlässigung zu paradoxen Lösungen führen kann. So ließe sich die Schutzaufgabe, einen Kunden vor einem Sprengstoffattentat auf ein Flugzeug oder vor einer Entgleisung des ICE zu bewahren, schlicht dadurch lösen, dass von der Reise abgeraten wird. Dadurch entstünde dem Kunden aber ebenfalls ein Schaden, nämlich der durch die Reise erwartete und ihm durch den Verzicht auf diese entgangene Nutzen.

Der Sicherheitsbedarf muss also den Gesamtnutzen für den Sicherheitsbedürftigen umfassen. Dies führt zum Begriff des Wagnisses. Als die für unsere Betrachtung nützlichste Definition von „Wagnis“ betrachten wir, auf einen bestimmten Zustand bezogen, das Wagnis als Produkt aus den Kosten, den dieser Zustand verursacht, und der





Wahrscheinlichkeit, dass dieser Zustand erreicht wird. Kosten können auch negativ sein. Damit sind sie Nutzen. Der Begriff „Wagnis" umfasst beide Vorzeichen der Kosten.[10] Als eine Funktion eines Zustands z, dessen Kosten k und dessen Eintrittswahrscheinlichkeit P ist das Wagnis w damit $w(z) := k(z)P(z)$.

Über alle relevanten Zustände hinweg ist das Gesamtwagnis W damit der Erwartungswert der Kosten:[11]

$$W := \sum_{z \in Z} w(z)$$

Damit lässt sich „Sicherheit" schlicht so definieren, dass für einen zukünftigen Zeitabschnitt das Wagnis einen positiven Wert annimmt, also die Chance das Risiko überwiegt. Sicherheit ist gegeben, wenn für einen definierten, zukünftigen Zeitabschnitt das Gesamtwagnis W positiv ist.





Wichtig für die Anwendung dieser Definition ist, dass nicht die nominellen, sondern die von dem Schutzbedürftigen eingeschätzten realen Kosten und Nutzen angesetzt werden. Eine Konstellation, in der mit einer Wahrscheinlichkeit von 0,9 ein Verlust von 10,- Euro und der Gewinn von 100.000,- Euro mit einer Wahrscheinlichkeit von 0,1 eintritt, ist nominell mit einem W von 9.991 Euro (= –10,- Euro * 0,9 + 100.000,- Euro * 0,1) eigentlich sicher. Für Menschen, die nur 10,- Euro besitzen, wiegt deren Verlust aber viel schwerer als für Reiche. Die realen Kosten sind also viel höher als die nominellen. Deshalb muss es den Menschen als Schutzbedürftige selbst überlassen werden, Kosten und Nutzen zu bewerten statt nur die nominellen Werte anzusetzen.[12]

Weiter wichtig für die Definition des Sicherheitsbedarfs ist die Eingrenzung des Zeitabschnitts, für den er gedeckt werden soll. Denn wird keine zeitliche Grenze gesetzt, wird jeder physikalisch mögliche Zustand irgendwann mit Sicherheit erreicht.

Obwohl es oft schwierig ist, sowohl die Eintrittswahrscheinlichkeit von Zuständen als auch deren Kosten zuverlässig abzuschätzen, hat diese Definition doch den Vorteil, dass sie das Wagnis in Zahlen ausdrückt, mithilfe derer eine Verständigung erleichtert würde. Dies ist im Dialog von Schutzbedürftigem und Schützer zwingend notwendig. Die Eintrittswahrscheinlichkeit ist dimensionslos. Daher trägt W die Dimension der Wäh-

10 Nach DIN 2005 bzw. DIN 820-120 umfasst der Begriff des Wagnisses sowohl Kosten als auch Nutzen. Das Wagnis wird als „Risiko" bezeichnet, wenn die betrachteten Zustände nur Kosten, als „Chance", wenn sie nur Nutzen bewirken.

11 In der Statistischen Entscheidungstheorie (Berger 1985) wird der Erwartungswert der Kosten als „Risiko" definiert. Die Kosten unterschiedlicher Zustände können unterschiedliche Vorzeichen haben, sodass in der Erwartungswertbildung Kosten und Nutzen miteinander verrechnet werden. In Bezug auf die Sicherheit ist eine solche Aufrechnung von Kosten und Nutzen juristisch nicht unproblematisch (vgl. den Beitrag von Vieweg in diesem Band).

12 In der Statistischen Entscheidungstheorie (Berger 1985) werden die monetären Kosten mittels einer sogenannten „utility function" im Allgemeinen nichtlinear abgebildet, um eine derartige Bewertung vorzunehmen.





rung, in der die Kosten für den Schutzbedürftigen anfallen. Diese Währung muss nicht zwingend die Dimension von Geld haben, sondern kann auch ein ideeller Wert sein. Sie bildet aber die Basis für das Entgelt, das der Schutzbedürftige dem Schützer für seine Leistung entrichtet. Deshalb wird eine Umrechnung in Geldwert aus praktischen Gründen nie ganz zu vermeiden sein.

2.2.3 DIE LEISTUNG DES SCHÜTZERS

Die Dienstleistung des Schützers besteht darin, den Sicherheitsbedarf des Schutzbedürftigen zu befriedigen. Obwohl Sicherheit – über das Wagnis ausgedrückt – auch den Nutzen einbezieht, ist der Schützer nicht für die Mehrung des Nutzens, sondern ausschließlich für das Abwenden von Schaden zuständig. Bei der Planung und Ausführung dieser Maßnahmen muss er nur Sorge tragen, dass der vom Kunden intendierte Nutzen nicht über ein möglicherweise notwendiges Maß hinaus vermindert wird. Um Schaden vom Schutzbedürftigen abzuwenden, hat der Schützer grundsätzlich drei Möglichkeiten, die einzeln oder gemeinsam genutzt werden können:[13]

1. die Verwundbarkeit mindern (an den verwundbaren Flanken),
2. die Gefährdungsausbreitung hemmen (am Übertragungsweg) und
3. den Gefährder neutralisieren.




Diese drei Angriffspunkte für den Schutz orientieren sich an der Wirkungskette vom Gefährder bis zum Schutzbedürftigen.[14] Diese Kette lässt sich unterbrechen, wenn an einem Glied vollständiger Erfolg erzielt wird. In aller Regel ist ein solch hundertprozentiger Erfolg an einer Stelle nur mit immens hohem Aufwand zu erreichen. Erfolg versprechender ist es, mit dem vom Schutzbedürftigen gezahlten Entgelt die Schutzleistung auf alle drei Stufen zu verteilen. Jede einzelne Stufe wird für sich nicht die höchste Sicherheit bieten. Durch ihre Verkettung ist der Erfolg aber höher als wenn der erlaubte Aufwand nur in einer der Stufen aufgebracht werden würde (Pareto-Prinzip). Problematisch hierbei ist, dass die vom Schutzbedürftigen „gefühlte" Sicherheit als am höchsten empfunden wird, wenn die direkten Flanken der Verwundbarkeit gehärtet sind.[15] Hier

---

13 Beyerer 2009.

14 Auch wenn der Gefährder einen Schaden nur androht, entsteht für den Schutzbedürftigen ein Schaden, nämlich der durch die Furcht vor Schädigung angerichtete.

15 Neben der ingenieurmäßigen Definition eines Wagnisses analog zum Risikobegriff der Statistischen Entscheidungstheorie (Berger 1985) ist der Risikobegriff im Kontext der Sicherheit vielschichtiger, wenn zusätzlich auch die Wahrnehmung von Risiko durch einzelne Menschen, Gruppen oder die ganze Gesellschaft einbezogen werden (Renn 2008, Renn/Walker 2008, Renn et al. 2007).





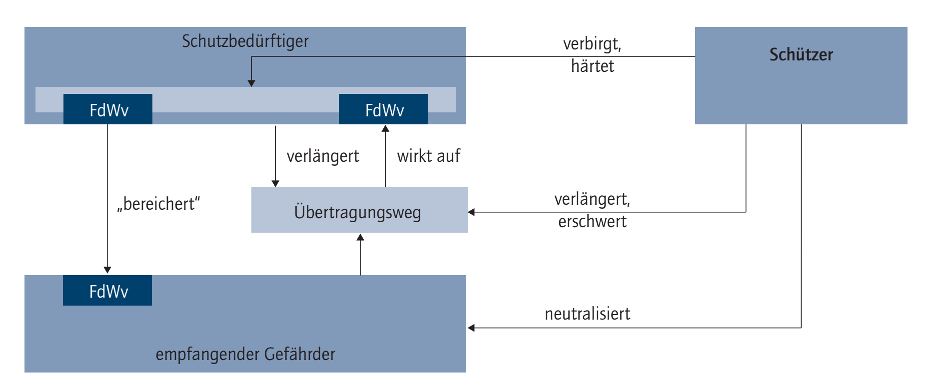
ist die höchste Sichtbarkeit der Sicherheit gegeben, auch wenn dies nicht unbedingt tatsächlich die höchste Sicherheit bietet. Abbildung 9 (siehe unten) gibt anhand des Basis-Systemmodells eine Übersicht über die Wirkungsmöglichkeiten des Schützers.

Die Härtung der verwundbaren Flanken wurde bereits im Abschnitt 2.2.1 anhand von Beispielen beschrieben (äußere Härtung, zum Beispiel durch Empfehlung eines Helms, innere Härtung, zum Beispiel durch Schutzimpfung). Diese Härtung wird immer direkt am Schutzbedürftigen und nicht selten – auf Anraten des Schützers – vom Schutzbedürftigen selbst vorgenommen.

Das Hemmen der Gefährdungsausbreitung kann geschehen durch die Verlängerung oder allgemeine Erschwerung des Übertragungswegs. Eine Möglichkeit dazu ist der bereits in Abschnitt 2.2.2 erwähnte Rat an den Schutzbedürftigen, sich vom Gefährder fernzuhalten. Die Hemmung der Gefährdungsausbreitung kann natürlich auch direkt am Übertragungsweg vorgenommen werden, ohne dass der Schutzbedürftige ausweichen muss. Beispielsweise kann der Schützer über einem Bürgersteig ein Fangnetz aufspannen, welches verhindert, dass herabfallende Dachziegel Passanten treffen. Im Unterschied zur Härtung verwundbarer Flanken, die auf individuelle Schutzbedürftige bezogen ist (hier zum Beispiel durch das Tragen von Helmen), wirkt diese Maßnahme auf eine ganze Klasse von Schutzbedürftigen.




Abbildung 9: Wirkung des Schützers auf Schutzbedürftigen, Übertragungsweg und Gefährder



Im Folgenden soll das Paket der Schutzmaßnahmen orientiert an der in Abschnitt 2.2.2 getroffenen grundsätzlichen Unterscheidung zwischen gewollter (Schaden als Mittel oder als Zweck) und ungewollter Gefährdung (Schaden durch Naturereignisse oder durch Fahrlässigkeit von Menschen) differenziert werden. Die Darlegung beginnt mit dem strukturell einfachsten Fall.





2.2.3.1 SCHUTZMASSNAHMEN BEI UNGEWOLLTER GEFÄHRDUNG DURCH NATUR-EREIGNISSE

Naturereignisse mit Schadenspotenzial wie Unwetter, Überschwemmungen oder Erdbeben können mit genügender Kenntnis der Naturgesetze und sorgfältigen, hinreichend dichten Messungen vorhergesagt werden. Die Härtung der verwundbaren Flanken bzw. die Erschwerung des Übertragungswegs geschieht entsprechend langfristiger Vorhersagen für jeweilige Risikogebiete und individuell für die erwartete Schadenswirkung (Deiche, Dämme, stabile Bebauung usw.) Kurzfristige Vorhersagen können insbesondere herangezogen werden, um den Übertragungsweg zu verlängern. Beispiel ist die rechtzeitige Information über einen drohenden Tsunami, nach der Menschen rasch ins höher gelegene Hinterland ausweichen können. Hier ist es wesentlich, dass sich die Information über eine drohende Gefahr schneller ausbreitet als die Gefahr selbst, was durchaus eine technische Herausforderung darstellt.

Das Neutralisieren von potenziell schädlichen Naturereignissen an der Quelle hängt von den technischen Möglichkeiten ab. Obwohl im Prinzip in vielen Fällen denkbar, kann dies de facto beliebig schwierig und aufwendig bis praktisch unmöglich sein. In der hier vorgenommenen, abstrakten systemtheoretischen Behandlung ist diese Form der Neutralisierung allerdings ohne strukturelle Besonderheit.




2.2.3.2 SCHUTZMASSNAHMEN BEI UNGEWOLLTER GEFÄHRDUNG DURCH MEN-SCHEN

Die Wahrscheinlichkeit fahrlässigen Verhaltens von Menschen lässt sich auf der einen Seite statistisch ermitteln und daraus lassen sich wiederum Prognosen für die Wahrscheinlichkeit des Auftretens ableiten. In diesem Fall besteht, was die Maßnahmen zur Härtung verwundbarer Flanken und das Hemmen der Gefährdungsausbreitung angeht, kein prinzipieller Unterschied zu Naturereignissen. Denn die Zufallsprozesse sind mehr oder weniger gut vorhersagbar.

Beim Neutralisieren des fahrlässigen Menschen als Gefährder kann jedoch auf der anderen Seite von dem besprochenen Umstand Gebrauch gemacht werden, dass Fahrlässigkeit für den, der sie sich leistet, zunächst Kosten spart. Der Schützer kann daher den fahrlässigen Gefährder mit Kosten beaufschlagen. Dies sieht unser Rechtssystem regelmäßig vor, indem vom fahrlässigen Gefährder ein Schadensersatz verlangt wird. Dieser wirkt zunächst erst nach Schadenseintritt, entfaltet aber dann eine erzieherische Wirkung, die den potenziell Fahrlässigen in Zukunft eine andere Kosten-/Nutzenrechnung aufmachen lässt.

Eine technische Möglichkeit besteht darin, Indikatoren für sich anbahnende Fahrlässigkeit zu finden, die technisch messbar sind. Menschen könnten dann rechtzeitig gewarnt werden, bevor sie in einen Zustand erhöhter Fahrlässigkeitsneigung gelangen, so zum





Beispiel durch Ermüdungswarnungen, wie sie in sehr einfacher Form durch den sogenannten Totmannschalter in Triebwagen der Bahn schon seit Langem realisiert sind und neuerdings durch die etwas feiner differenzierende Analyse der Lenkbewegungen für Kfz-Fahrer realisiert werden.

2.2.3.3 SCHUTZMASSNAHMEN BEI GEWOLLTER GEFÄHRDUNG ALS MITTEL

Da hier der Gefährder bewusst einen Schaden herbeiführen oder glaubhaft androhen will, wird er sich die schwächste Flanke der Verwundbarkeit und die lohnendste Flanke der Wertveräußerung aussuchen. Die günstigste Maßnahme an diesen Flanken ist es, sie möglichst verborgen zu halten bzw. den Gefährder über deren Festigkeit zu täuschen. Da dies nicht durchgehend möglich bzw. unsicher ist, da in der Regel nicht bekannt ist, was der Gefährder weiß, wird ein möglichst durchgängiges Härten dieser Flanken nicht vermeidbar sein. Hier besteht auch das Problem, dass man als Schutzbedürftiger dem Schützer gegenüber seine Verwundbarkeit offenlegen, vor potenziellen Gefährdern aber verborgen halten sollte. Dies verlangt erstens ein besonderes Vertrauensverhältnis zum Schützer im Falle dieser Gefährdungsklasse und zweitens einen sicheren Kommunikationskanal zu diesem.




Der Vorteil gegenüber der Gefährdung durch Fahrlässigkeit ist, dass der Schützer aus dem ihm bekannten Wertvorrat des Schutzbedürftigen schließen kann, welche potenziellen Gefährder infrage kommen. Sollte er deren Schädigungspotenzial kennen, kann er die passenden Flanken der Verwundbarkeit härten, die erwarteten Übertragungswege blockieren und die Gefährder gezielt neutralisieren. Allerdings haben wir es hier nicht, wie in den zuvor genannten Fällen, mit Zufallsprozessen, sondern mit Absicht zu tun. Aus spieltheoretischer Sicht handelt es sich beim Umgang mit Zufallsprozessen um ein „Spiel gegen die Natur", das – vom Eintreten bis dato nicht bekannter Einflüsse abgesehen – auf lange Sicht gewonnen werden kann. Dagegen ist die Bekämpfung eines absichtlichen Gefährders ein „Spiel gegen einen intelligenten Gegner", dessen Ergebnis immer offen ist.

So ist auch das Neutralisieren des wollenden Gefährders zwar dahingehend leichter als das des fahrlässigen, dass er leichter identifiziert werden kann. Allerdings ist es insofern schwerer, als in der Regel dieselbe Maßnahme nicht zweimal angewendet werden kann.

Hat der Gefährder, wie in diesem Abschnitt angenommen, jedoch ein materielles Interesse, dann kann man ihn bei den Kosten „packen" und nach Abbildung 5 entweder den Schutzbedürftigen unempfindlicher machen, sodass er erst bei höherer Schadensandrohung nennenswerte Werte veräußern würde oder man kann die Schaden-zu-Kosten-Relation für den Gefährder verschlechtern. Die letztere Option kann neben





der erwähnten Härtung der Flanken und der Erschwerung des Übertragungswegs auch beispielsweise durch kontinuierliche Beobachtung und damit einen gewissen Verfolgungsdruck erreicht werden – wiederum ein Mittel zur Neutralisierung des Gefährders. Letztlich kann man mit einem Gefährder dieser Kategorie auf irgendeine Weise „ins Geschäft kommen", da er ein materielles Interesse hat.

2.2.3.4 SCHUTZMASSNAHMEN BEI GEWOLLTER GEFÄHRDUNG ALS ZWECK

Auch hier wird sich der Gefährder die schwächste Flanke suchen, sodass man, wie im Szenario von 2.3.3.3, entweder alle Flanken genügend härten oder verbergen muss. Dasselbe gilt für den Übertragungsweg. Die Flanken der Wertveräußerung spielen hier allerdings wie bei 2.2.3.1 und 2.3.2.2 keine Rolle.

Was das Neutralisieren von potenziellen Gefährdern angeht, so kann es ebenfalls – in engen Grenzen – gelingen, den möglichen Personenkreis einzugrenzen. Aber auch hier hat man es mit einem intelligenten Gegner zu tun, der sich in der Regel geschickt verborgen hält.




Was den Umgang mit Gefährdungen dieser Kategorie besonders schwierig macht, ist erstens, dass die Gefährder keine proportionale Kosten-/Nutzen-Kalkulation anstellen, sondern maximalen Schaden anrichten, wenn sie die Möglichkeit dazu haben. Die Neutralisierung solcher potenzieller Gefährder kann dadurch geschehen, dass die Kosten zur Beschaffung von Schadmitteln in die Höhe getrieben werden, dass sie mit den Schadmitteln, die Gefährder sich leisten können, keinen für sie ausreichenden Schaden anrichten können und sie deshalb die Schädigung unterlassen (siehe Abbildung 6). Ist die Veranlagung zur Schädigung als Zweck allerdings vorhanden, besteht große Gefahr, dass sie sich findig Wege sucht, an genügend mächtige Schadmittel zu gelangen.

2.2.4 EIGENSCHAFT VON SCHUTZPROZESSEN

Abbildung 10 veranschaulicht wesentliche Eigenschaften der möglichen Maßnahmen des Schützers zur Beherrschung von Gefährdungen, die dem Schutzbedürftigen drohen, gegliedert nach den Gefährdungskategorien. Während bei der gewollten Gefährdung die schwächste Flanke die Verwundbarkeit bestimmt, da der Gefährder sich diese suchen wird, kann man bei der ungewollten Gefährdung abschätzen, welche Gefährdungen wahrscheinlich drohen, und die dagegen empfindlichen Flanken der Verwundbarkeit bevorzugt härten.

Während der Schutzprozess gegenüber ungewollten Gefährdungen konvergieren kann, da (sprunghafte Veränderungen der Natur ausgeschlossen) mit längerer Beobachtung immer genauere Kenntnisse über die zu erwartenden zufälligen Gefährdungen gewonnen werden können, oszilliert der Schutz gegen gewollte Gefährdungen. Denn





hier hat man es mit einem planenden Gefährder zu tun, der immer danach trachtet, Schwächen im Schutz zu identifizieren und auszunutzen, worauf nach gewisser Zeit auch der Schützer reagiert, worauf wiederum der Gefährder reagiert usw. Spieltheoretisch betrachtet, ist der Schutz vor ungewollter Gefährdung ein „Spiel gegen die Natur", während es sich beim Schutz vor gewollter Gefährdung um ein „Spiel gegen einen Gegner" handelt (siehe Abschnitt 2.2.3.3).

Eine Brücke zwischen der gewollten und ungewollten Gefährdung wird, zumindest, was die Schutzmaßnahmen angeht, zwischen der gewollten Gefährdung als Mittel und der ungewollten Gefährdung durch Fahrlässigkeit geschlagen. Bei beiden Kategorien lassen sich die Menschen, die hier als Gefährder auftreten, durch eine mit dem Schadenspotenzial wachsende Kostenbeaufschlagung in ihrer Gefährdung einschränken. Für den materiell orientierten Gefährder büßt die Gefährdung dadurch an Lukrativität ein. Für den fahrlässigen Gefährder kann sich der Aufwand für die Gefährdungsvermeidung lohnen.

Dagegen ist die Natur völlig unempfindlich gegen Kostenbeaufschlagung. Und der wollende Gefährder, der den Schaden als Zweck sieht, wird alles daran setzen, die für die Mindestschädigung nötigen Kosten aufzubringen und, wenn ihm dies gelungen ist, maximalen Schaden zu erzeugen.





Abbildung 10: Eigenschaft der Maßnahmen zur Beherrschung der Gefährdungskategorien

Gefährdung
gewollt
ungewollt
als Zweck
als Mittel
durch Fahrlässigkeit
durch Naturereignisse
durch schadensproportionale Kostenbeaufschlagung der Gefährdung beherrschbar
schwächste Flanke bestimmte Verwundbarkeit
am wahrscheinichsten erreichte Flanke bestimmt Verwundbarkeit
Schutzprozess osziliiert
Schutzprozess konvergiert





2.3 VON DER SYSTEMANALYSE ZUM SYSTEMDESIGN: FAZIT UND ÜBERLEITUNG

Für eine Systemanalyse von Sicherheitsproblemen mit dem Ziel, Schutzsysteme optimal zu gestalten, wurde ein Basissystemmodell bestehend aus den drei Elementen Schutzbedürftiger, Schützer und Gefährder aufgestellt. Diese Elemente, die ihrerseits wieder Systeme sein können, sind als Rollen zu verstehen, die über definierbare Schnittstellen miteinander in Verbindung treten. Die Schnittstelle zwischen Schutzbedürftigem und Schützer ist durch eine Dienstleistungsbeziehung gekennzeichnet, bei welcher der Schutzbedürftige seinen Sicherheitsbedarf äußert und der Schützer diesen entsprechend befriedigt. Zwischen beiden muss eine Art Schutzvertrag bestehen, der insbesondere auch die Vertraulichkeit der Information über die Verwundbarkeit des Schutzbedürftigen sicherstellt. Sicherheit wird als gegeben erachtet, wenn für einen definierten und beschränkten Zeitraum das Wagnis als Summe der Produkte der Wahrscheinlichkeit des Eintretens künftiger Zustände und deren Kosten bzw. Nutzen (die Summe von Risiko und Chance) positiv ist.

Die Verwundbarkeit des Schutzbedürftigen wird in sogenannten „Flanken der Verwundbarkeit" ausgedrückt. Diese sind die Angriffspunkte für den Gefährder. Wir unterscheiden zwischen „gewollter" und „ungewollter Schädigung". Die ungewollte Schädigung, die durch Naturereignisse mit Gefahrpotenzial (zum Beispiel Unwetter) oder Fahrlässigkeit von Menschen erfolgt, trifft die Flanken der Verwundbarkeit zufällig. Die gewollte Schädigung hingegen trifft diese Flanken gezielt entweder mit dem Zweck, von dem Schutzbedürftigen gegen dessen Willen einen materiellen Wert zu empfangen (zum Beispiel durch Raub), oder um durch die Schädigung selbst eine ideelle Genugtuung zu erfahren. Im ersten Fall wird die Schädigung bzw. deren Androhung als Mittel eingesetzt, im zweiten Fall ist sie der Zweck. Im ersten Fall geht der Gefährder aufwandssparend nach dem Minimalprinzip vor und schädigt nur in dem Maße, in dem er es für nötig hält. Im zweiten Fall sucht der Gefährder bei gegebenem Aufwand maximalen Schaden.



Der Schützer hat im Wesentlichen drei Möglichkeiten der Einwirkung, um den Sicherheitsbedarf des Schutzbedürftigen zu befriedigen: Er kann direkt am Schutzbedürftigen dessen Flanken der Verwundbarkeit härten, er kann die Ausbreitung der Gefährdung auf dem Übertragungsweg zwischen Gefährder und Schutzbedürftigem hemmen und er kann den Gefährder neutralisieren. Nach dem Pareto-Prinzip kann es wirkungsvoller sein, den Schutzaufwand auf alle drei Stufen zu verteilen als ihn auf eine Stufe zu konzentrieren und die anderen zu vernachlässigen.

Bei der Härtung der verwundbaren Flanken sollte nur bei ungewollter Gefährdung eine Auswahl entsprechend der Schädigungswahrscheinlichkeit getroffen werden. Bei gewollter Gefährdung wird sich der Gefährder bewusst die schwächste Flanke suchen, sodass die Schwächen entweder geschickt verborgen oder alle Flanken gleichmäßig gehärtet werden müssen.





Im Falle gewollter Schädigungen, die als Mittel eingesetzt werden, kann der Gefährdungsgrad durch Hochtreiben des Aufwands für den Gefährder kontinuierlich gesenkt werden, da solche Gefährder Kosten und Nutzen kalkulieren. Im Falle gewollter Schädigung als Zweck kann durch Steigerung der Kosten die Gefährdung entweder komplett unterdrückt werden, wenn der Kostengrenzwert erreicht ist, oder die Maßnahme bleibt ohne Wirkung, wenn der Kostengrenzwert nicht erreicht wird.

Während der Schutzprozess gegenüber ungewollten Gefährdungen als „Spiel gegen die Natur" konvergieren kann, oszilliert der Schutz gegen gewollte Gefährdungen als „Spiel gegen einen Gegner" immer.

Das in diesem Kapitel beschriebene Basissystemmodell dient nachweislich der systematischen Lösung von Sicherheitsproblemen. Es weist Systemelementen, welche selbst auch Systeme sein können, definierte Rollen (Gefährder, Schutzbedürftiger und Schützer) zu. In der Folge werden die Wechselbeziehungen zwischen den durch Rollen attribuierten Systemelementen (Gefährder und Schutzbedürftiger, Schutzbedürftiger und Schützer, um nur einige zu nennen) untersucht. Daraus ergeben sich eine Reihe beschriebener Lösungsansätze.




Doch was passiert, wenn sich die Systemgrenzen und/oder die Systemelemente verändern? Systeme mit wachsender Komplexität bzw. mit einer erhöhten Dynamik unterliegen einer Expansion ihrer Systemgrenzen sowie einer Zunahme der Wechselwirkungen der Systemelemente. Das folgende Beispiel verdeutlicht, dass mit zunehmender Komplexität auch die Dynamik der zu betrachtenden Systeme selbst wächst, was systemische Problemlösungsstrategien sicher nicht vereinfacht.

Vor einigen Jahren im Herbst kam es in Nordrhein-Westfalen zu erheblichen Verspätungen im S-Bahn-Nahverkehr. Als Begründung wurde von den zuständigen Stellen damals „nasses Herbstlaub" genannt. Den Ausgangspunkt für diese Schwierigkeiten bildete die Entwicklung eines neuen S-Bahn-Triebwagens, dessen Konstruktions- und Entwicklungsziele sich über „umweltfreundliche" Merkmale wie „Leichtigkeit", „Schnelligkeit", „Zuverlässigkeit", „erhöhte Sicherheit", „geringster Energieverbrauch" sowie „wartungs- und instandhaltungsarm" charakterisieren sollten. Dieser sehr leichte Zug kam bei all seinen Bremsvorgängen auf dem nassen Laub ins Rutschen, während die traditionellen schweren Züge die Blätter auf den Schienen zermalmten. Dies stellte in hohem Maße eine Gefährdung dar. Das Rutschen der Räder auf den Schienen verursachte einen einseitigen Abrieb, der bei mehrmaligem Bremsen zu unrunden Rädern führte. Die daraus resultierenden verschlechterten Laufeigenschaften zeigten Auswirkungen auf das gesamte Fahrgestell. Häufige Reparaturen der Fahrgestelle wurden als zwingende Maßnahme zur Beseitigung der Gefahrenquellen, die es ursprünglich eigentlich zu vermeiden galt, notwendig. Hinzu kam, dass aufgrund des ursprünglich prognostizierten geringen Instandhaltungsaufwands die Verantwortlichen keine Fahrgestelle mehr lagerten, um die Lagerkosten für das Unternehmen zu minimieren. Aus diesem Grunde ließen sich die





notwendig gewordenen Fahrgestellwechsel, welche bestehende Gefährdungen vermeiden sollten, nicht durchführen. Eine Vielzahl von neuen Zügen stand im Depot und dies führte zu Kapazitätsengpässen im Nahverkehr in Nordrhein-Westfalen.

Zur kurzfristigen Überbrückung dieser Engpässe wurden Züge des alten (schwereren) Modells bei anderen Verkehrsverbünden geliehen und wieder eingesetzt, was zu zusätzlichen Kosten führte. Gleichzeitig wurde an einer langfristigen Lösung gearbeitet: Das Anbringen eines Sandstrahlgebläses an der Front des Zuges bzw. eines Laubgebläses sollte das nasse Laub von den Schienen entfernen. Allerdings führten diese Maßnahmen, die in anderen Bundesländern erfolgreich eingesetzt wurden, nicht zum gewünschten Erfolg: Während der Sand solcher Sandstrahlgebläse zwar Laub entfernte, durch den erhöhten Abrieb aber zur Beeinträchtigung sowohl der Schiene als auch des Rades und somit der Sicherheit führte, verwirbelte das Laubgebläse lediglich die Blätter. Im Gegensatz zur Situation in NRW funktionierte dieses Laubgebläse bei den Nahverkehrsverbünden in Bayern, die ebenso in leichten Zügen ihre Zukunft sahen, einwandfrei.

Die Ursachen lagen allerdings nicht in der Konstruktion der Laubgebläse aus NRW, sondern in einer zu engen Betrachtung des Systems „leichter Zug auf herbstlichen Schienen". Ein Vergleich der verschiedenen Nahverkehrssysteme von Bayern und Nordrhein-Westfalen ergab, dass in NRW – im Gegensatz zu Bayern – fast 80 Prozent des Schienensystems von Lärmschutzwänden begrenzt wird. Bei Strecken ohne Lärmschutzwand – wie überwiegend in Bayern – trieb das Laubgebläse die Blätter zur Seite. Auf den Strecken in NRW flogen die Blätter aufgrund der Lärmschutzwände nicht weit genug ins Umfeld. Folglich führte die Entwicklung des Laubgebläses in Bayern zum Erfolg, weil die fehlenden Lärmschutzwände ganz andere Strömungsverhältnisse der Luft erzeugten als in Nordrhein-Westfalen.




Das Beispiel unterstreicht, dass die Berücksichtigung der Systemgrenzen für die effiziente Suche nach neuen Ideen von essenzieller Bedeutung ist. Zunächst den Lösungsraum sehr eng zu begrenzen, um darin Lösungsansätze zu generieren, ist genauso wichtig wie eine Untersuchung der gefundenen Lösungen auf ihre Praktikabilität und Fehlerfreiheit in größeren Lösungsräumen. Das Problem solcher expandierenden Systemgrenzen effizient zu lösen gewinnt zunehmend an Bedeutung und bedarf praktikabler Methoden und Verfahren zu seiner Unterstützung. Im folgenden Abschnitt wird daher untersucht, welchen Beitrag das System Engineering zur Systemanalyse „Sicherheit" leisten kann. Besonderes Augenmerk gilt hierbei den Systemgrenzen.

2.4 SYSTEMS ENGINEERING ALS BEITRAG ZUR SYSTEMANALYSE

Das „Systems Engineering" ist eine Disziplin zur systematischen Problemlösung, aber auch zum systematischen Nutzen unseres Wissens. Sie ist keine neue Wissenschaftsdisziplin, sondern leistet seit mehr als 50 Jahren einen Beitrag zur Komplexitätsreduzierung. Das Systems Engineering ist eine generelle Methode zur Analyse komplexer Situationen,

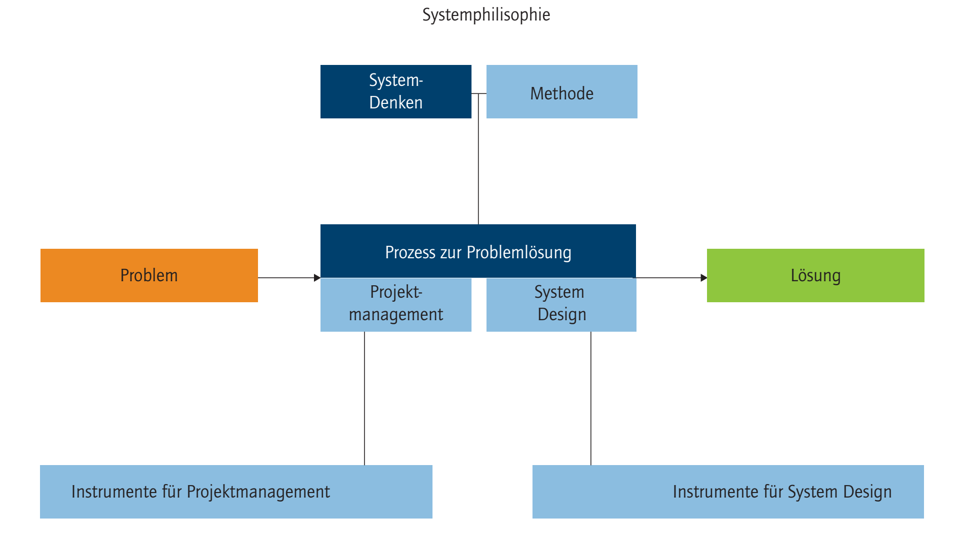




Prozesse oder Strukturen und ist nutzbar für die Analyse wie auch für die Modellierung und Gestaltung von Systemen und Subsystemen. Folglich müsste es auch für die Lösung von komplexen sicherheitsrelevanten Fragenstellungen geeignet sein. Jedoch gibt es verschiedene Vorgehensweisen des Systems Engineering in der Literatur. Diese Vielfalt und die damit einhergehende mangelnde Transparenz haben dazu geführt, dass das Systems Engineering sowohl als generelle Methode als auch zur Lösung sicherheitsrelevanter Fragestellungen kaum noch Anwendung findet.
Eine Analyse der von Arlt[16] vorgenommenen Clusterung der Ansätze des Systems Engineering nach ihren Denkmodellen, Vorgehensweisen, Grundprinzipien, den angewandten Methoden und der Organisation zeigt, dass ein genereller bzw. universeller Ansatz des Systems Engineering, der auch für das Produktsystem „Sicherheit“ geeignet ist, fehlt. Grundsätzlich wird jedoch deutlich, dass die von Haberfellner[17] vorgeschlagene Grundeinteilung der Systemphilosophie geeignet ist (siehe die nachfolgende Abbildung).

Abbildung 11: Systemphilosophie nach Haberfellner



Haberfellner zufolge kann die Systemphilosophie zum Lösen jeglicher Art von Problemen genutzt werden. Als Voraussetzung dafür ist es zunächst erforderlich, ein Denkmodell, das „System-Denken“, zu entwickeln und darauf aufbauend eine „methodische Vorgehensweise“ abzuleiten. Die Basis dieses Denkmodells bildet der Ansatz, alles, was uns

16 Arlt 1999.
17 Haberfellner 1999.





umgibt, als Systeme bzw. Subsysteme und deren Elemente aufzufassen. Dabei ist die Art des jeweiligen Systems zunächst nicht von Bedeutung. Haberfellner bedient sich im Rahmen der „methodischen Vorgehensweise“ zweier wesentlicher Aspekte: dem „Design des Systems“ selbst und dem „Projektmanagement“ (wie in Abbildung 11 dargestellt). Im Rahmen dieser beiden Schwerpunkte werden jeweils verschiedene Instrumente genutzt. Die Kombination der einzelnen Instrumente ist nach Haberfellners Auffassung von dem zu lösenden Problem abhängig.[18]

Haberfellner hat bewiesen, dass nicht jedes spezifische Problem einer spezifischen Problemlösung bedarf, sondern dass mit der Anwendung einer generellen Methode bei gleichzeitiger Nutzung spezifischer Instrumente jedwede Art von Problemlösung möglich ist. Somit kann auf eine Vielzahl von Methoden und Verfahren, die ausschließlich entwickelt worden sind, um spezifische Probleme zu lösen, verzichtet werden.

Grundsätzlich kann dieser Vorgehensweise von Haberfellner zugestimmt werden. Dennoch fehlt ein wichtiger Aspekt bei Haberfellners Ansatz: Bevor das Problem analysiert werden kann, muss exakt das betrachtete System in Bezug zu seiner Systemumgebung abgegrenzt werden. Die Notwendigkeit dieser Vorgehensweise wurde an dem Beispiel des öffentlichen Nahverkehrs in Nordrhein-Westfalen deutlich. Hier konnte eine zufriedenstellende Lösung zur Gewährleistung der Sicherheit und Zuverlässigkeit im Herbst nur durch die Erweiterung der Systemgrenzen gefunden werden.





2.4.1 GENERIC SYSTEMS ENGINEERING (GSE) ALS ANSATZ ZUR GESTALTUNG VON SICHERHEITSSYSTEMEN

Grundsätzlich ist es notwendig, einen Ansatz zu entwickeln, der es ermöglicht, fachdisziplinübergreifend Systeme zu beschreiben und die Vielzahl der bestehenden Vorgehensmodelle des Systems Engineering zu vereinheitlichen. Aus diesem Grund entwickelten Sitte/Winzer ein generisches Vorgehensmodell bei Beibehaltung des Denkmodells von Haberfellner. Der Generic Systems Engineering (GSE)-Ansatz beruht auf der Systemtheorie und damit auf dem Systems Engineering (SE). Dabei wurde das vorhandene Potenzial des Systems Engineering zur umfassenden Problemlösung weiterentwickelt. Das Generic Systems Engineering (GSE) unterstützt basierend auf dem Systemdenken die Analyse, die Modellierung und die Gestaltung komplexer Zusammenhänge, Prozesse oder Strukturen.

Dabei ist es wichtig, dass die Spezifik des zu lösenden Problems zunächst nicht von Interesse ist, sondern die Identifikation des Systems, an das das Problem angelagert sein könnte, im Vordergrund steht. Das setzt voraus, dass eine Interessenfokussierung stattgefunden hat. Ist zum Beispiel die Funktionssicherheit des Bremssystems eines Autos der Betrachtungsgegenstand und wird in der Folge nur das Bremssystem in Wech-

[18] Vgl. Sitte/Winzer 2004.





selwirkung mit den anderen Teilsystemen des Autos betrachtet, kann im Sinne einer Komplexitätsreduktion zunächst die Wechselwirkung mit der Umwelt, zum Beispiel die Auswirkung von verschiedensten Straßenbelägen auf die Sicherheit des Bremssystems vernachlässigt werden. Das bedeutet nicht, dass diese Betrachtung zu einem späteren Zeitpunkt erfolgt. Der GSE-Ansatz setzt sich aus den folgenden drei Teilen zusammen:

1. die Beschreibung des Systems,
2. die einzelnen Schritte des Systemdesigns,
3. die Kombination der Schritte des Systemdesigns.

Teil 1 (Beschreibung des Systems) des Generic Systems Engineering-Ansatzes umfasst:

- die Charakteristik des Systems,
- die Unterteilung des Systems in seine Subsysteme und Elemente,
- die Hierarchisierung des Subsystems,
- die Darstellung der Wechselbeziehungen zwischen den Subsystemen und den Elementen sowie den Subsystemen untereinander,
- die Charakteristik der Wechselwirkungen des Systems mit seiner Umwelt.



Vor der Zielsetzung eines generellen Lösungsansatzes erfolgt in diesem Zusammenhang keine detaillierte Zuordnung von bestimmten Rollen zu den Elementen, wie es in Abschnitt 3 vorgeschlagen wird, um ein Basismodell für das Produkt „Sicherheit" abzuleiten. Dennoch ist diese Modifizierung für eine gezielte Sicherheitsanalyse denkbar. Dabei ermöglichen die unterschiedliche Art und Weise der Clusterung der Subsysteme und die Betrachtung ihrer Wechselwirkungen unterschiedliche Sichtweisen auf das gleiche System. Dies kann verglichen werden mit der Schichtfotografie. Mit verschiedenen Filtern, wie zum Beispiel dem Einsatz von Blau- oder Gelbfilter, können verschiedenste Aspekte des gleichen Motivs deutlicher hervorgehoben werden. Die verschiedenen Sichtweisen ermöglichen, genauer zu erkennen, in welcher Art und Weise die Subsysteme funktionieren bzw. mit dem Gesamtsystem interagieren. Im Bezug auf Sicherheit ist ein mögliches „Filterset" der Safety- bzw. der Security-Blickwinkel auf ein und dasselbe System (zum Beispiel das System ICE, wie es im folgenden Abschnitt beschrieben ist), da die Sicherheit in einem System zwangsläufig beide Aspekte berücksichtigen muss.

Der zweite Teil (die einzelnen Schritte des Systemdesigns) des generellen methodischen Ansatzes des Systems Engineering lässt sich in drei Abschnitte untergliedern:

- den Zielbildungsprozess,
- den Analyseprozess
- und den Designprozess.





Nachdem die Systemgrenzen bekannt sind, können alle Anforderungen erhoben werden, die an dieses System gestellt werden. Dabei ist es besonders wichtig, nicht nur die Anforderungen selbst, sondern auch ihre Quellen eineindeutig zu erfassen. In einem Folgeschritt werden die Anforderungen grob geclustert. Dies ist die Voraussetzung für einen vereinfachten paarweisen Vergleich, der eine deutliche Reduktion der Anforderungsvielfalt ermöglicht. Im Ergebnis der vergleichenden Betrachtung ist erkennbar, welche Anforderungen ähnlich, gleich oder widersprüchlich sind. In einem weiteren Folgeschritt werden die Anforderungen nach Wichtigkeit bewertet. Das ist die Voraussetzung, um Ziele zu bilden. Der Zielbildungsprozess umfasst dabei die Auswahl und die Konkretisierung der Anforderungen, die umgesetzt werden sollen, wie auch die Art und Weise der Realisierung, das heißt, durch welche Maßnahmen diese Anforderungen umgesetzt werden. Der Zielbildungsprozess kann einseitig durch den Systembesitzer, aber auch in Form des Interessenabgleichs mit den Stakeholdern des Systems erfolgen. Nachdem die Ziele fokussiert sind, beginnt der spezielle Analyseprozess des Systems. Dabei werden die Subsysteme bzw. die Elemente und die Beziehungen zwischen den Subsystemen und deren Elementen genauer beleuchtet. Im Vordergrund der Analyse steht die Art und Weise der Wechselbeziehungen zwischen den einzelnen Subsystemen und Elementen.
Im Ergebnis der Analyse können sich erneut Präzisierungen für den Teil 1, die Definition des Systems, ergeben. Gleichzeitig bildet dieser Schritt die Basis für das sich anschließende Systemdesign, da nur die Kenntnis der Art und Weise des Zusammenwirkens aller Subsysteme untereinander die effiziente Gestaltung des Systems entsprechend der jeweiligen Zielvorgaben ermöglicht. Zielbildung, Analyse und Design bedienen sich dabei in Abhängigkeit des zu lösenden Problems unterschiedlicher Instrumente.




Die oben dargestellten Schritte des zweiten Teils des GSE-Ansatzes sind in unterschiedlicher Art und Weise miteinander kombinierbar. Das ist Gegenstand des dritten Teils des GSE-Ansatzes. Infolge der Anzahl der zur Verfügung stehenden Methoden sowie der verschiedenen Zielsetzungen ergeben sich unterschiedliche Varianten der Kombination von Teilschritten aus Teil 2 der Methodik. Die zeitlich-logischen Kombinationen dieser Teilschritte sind zu fixieren und als eine Art „Plan der Systemgestaltung", das heißt als Teil 3 des Systems Engineering-Vorgehens, schrittweise umzusetzen. Auch hierfür können unterschiedliche Instrumente genutzt werden. Das bekannteste Beispiel ist das Projektmanagement. Aber auch die Netzplantechnik oder der Balkenplan sind Instrumente, welche die Art und Weise des Problemlösungszyklus vorskizzieren. Dabei ist darauf zu achten, dass in bestimmten Zeitabständen der Stand der Planrealisierung geprüft bzw. präzisiert werden muss.

Im Folgenden werden die beiden Aspekte Systemgrenzen sowie die Strukturierung der Anforderungen, die, wie oben beschrieben, ein zentraler Bestandteil des GSE-Ansatzes ist, anhand von Beispielen verdeutlicht.





2.4.2 BEDEUTUNG DER SYSTEMGRENZEN FÜR DIE SYSTEMANALYSE „SICHERHEIT"

Vollkommene Sicherheit für alle Lebewesen und die Umwelt zu schaffen, ist bekanntermaßen nicht möglich. Das Produkt „Sicherheit" kann immer nur innerhalb eines begrenzten Systems erreicht bzw. sinnvoll angestrebt werden, da innerhalb eines Systems eine endliche Anzahl von Beziehungen bzw. Zusammenhängen und Elementen existiert, die es zu berücksichtigen gilt. Dennoch ist es von zentraler Bedeutung, diese Systemgrenzen nicht zu eng zu stecken und damit zwar auf der einen Seite eine überschaubare Anzahl an Beziehungen und Elementen zu erhalten, auf der anderen Seite aber zu stark zu vereinfachen und auf diese Weise die Tragweite einer Gefährdung zu unterschätzen.
Das ICE-Unglück in Eschede zeigt diesen Sachverhalt auf tragische Weise: Das Unglück betraf nicht nur den Zug und seine Insassen, sondern auch die Infrastruktur, Personen in der Umgebung, Wartungsmitarbeiter der Bahn etc. Infolgedessen wäre es zu wenig, das System, für welches das Konstruktions- und Wartungspersonal der Bahn zumindest annähernde Sicherheit gewährleisten soll, auf den Zug zu beschränken. Vielmehr müssen sowohl das direkte Umfeld des Zuges als auch das persönliche Umfeld der Reisenden und Mitarbeiter betrachtet werden.

Abbildung 12: System „Einzugsbereich ICE"



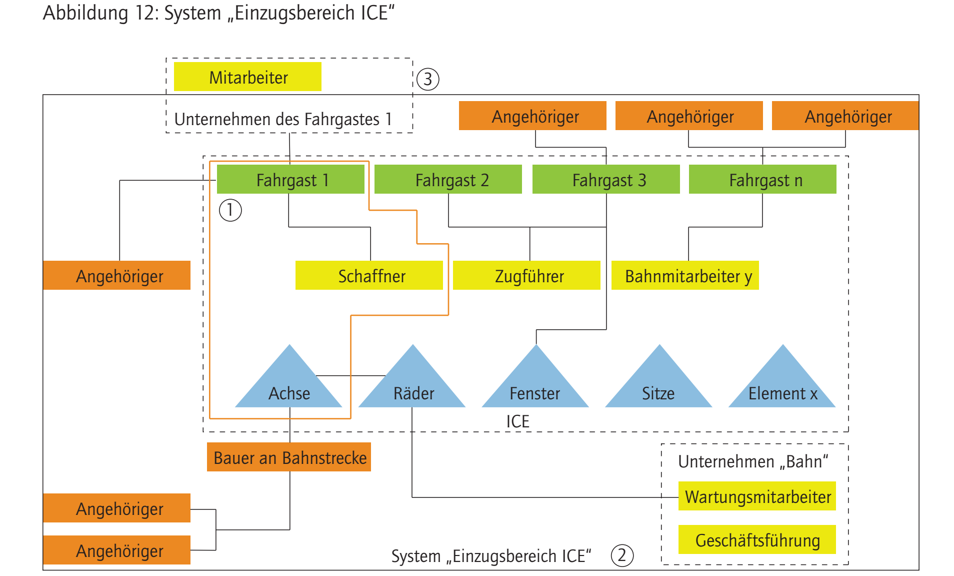







Abbildung 12 verdeutlicht anhand einiger exemplarischer Systemelemente und deren Beziehungen die Bedeutung der Systemgrenzen zur Abschätzung der Folgen eines derartigen Unfalls.

Mit „1" ist in diesem Zusammenhang das Teilsystem kennzeichnet, das im ersten Teil der Systemanalyse (vgl. Abschnitt 2.2) als Beispielsystem herausgegriffen wurde. Bei einer alleinigen Betrachtung dieses Teilsystems ist es, wie obige Abbildung veranschaulicht, nicht möglich, das ganze Ausmaß eines solchen Unfalls und somit auch das bestehende Risiko abzuschätzen. Es ist also nötig, sowohl das Gesamtsystem (hier mit „2" gekennzeichnet) zur umfassenden Risikoabschätzung als auch das (in diesem Fall auf einen Fahrgast als „Schutzbedürftigen" bezogene) Teilsystem zur Einschätzung des persönlichen Risikos zu analysieren.

Die Schwierigkeiten bei der Betrachtung eines weiter gefassten Systems liegen:





a) in der Zuweisung der jeweiligen Rollen („Schutzbedürftiger", „Gefährder" und „Schützer") zu den einzelnen Systemelementen, da in einem größeren System die einzelnen Elemente Bestandteile verschiedener Teilsysteme sein können und damit gleichzeitig verschiedene Rollen spielen können. Beispielsweise kann der Schaffner im Teilsystem eines Fahrgastes „Schützer", in seinem eigenen Teilsystem aber gleichzeitig „Schutzbedürftiger" sein.
b) in der Frage: „Wann ist das System groß genug?" bzw. „Wie viele Zwischenstufen bei indirekter Betroffenheit soll das System berücksichtigen?" Beispielsweise sind die Mitarbeiter eines im Zug verunglückten Firmenbesitzers durchaus indirekt von dem Unfall betroffen, können aber bei der Kalkulation des Risikos nur sehr schwer berücksichtigt werden (in Abbildung 11 mit „3" bezeichnet).
c) in der Analyse der zahlreichen Wechselbeziehungen zwischen den einzelnen Systemelementen und den verschiedenen Teilsystemen.
d) in der Analyse der zahlreichen Wechselbeziehungen zwischen dem System und seiner Umwelt.

Neben der eben beschriebenen Bedeutung der Systemgrenzen sowie der Schwierigkeiten, die beim Abgrenzen eines Systems auftreten, ist es von zentraler Bedeutung, sich mit den Anforderungen der „Schutzbedürftigen" bezüglich Sicherheit auseinanderzusetzen. Diese Anforderungen beziehen sich sowohl auf „Safety" als auch auf „Security", wobei der „Schutzbedürftige" meist keine Trennung der beiden Themenfelder vornimmt.





2.4.3 ANFORDERUNGSSTRUKTURIERUNG IN DER SYSTEMANALYSE „SICHERHEIT"

Die Sicherheit eines Zuges bzw. einer Zugreise, also eines Systems, ist für den einzelnen Reisenden bzw. „Schutzbedürftigen" eine grundlegende Anforderung. Um ein System aber anforderungsgerecht gestalten zu können, müssen zunächst die Anforderungen der relevanten Stakeholder an das jeweilige System bekannt sein. Um wiederum die Anforderungen der relevanten Stakeholder ermitteln zu können, müssen diese bekannt sein. In Bezug auf Sicherheit sind die relevanten Stakeholder, also die „Träger" einer Sicherheitsanforderung, die Schutzbedürftigen. In diesem Fall ist zwar beispielsweise der Gesetzgeber der Kommunikator einer solchen Sicherheitsanforderung, indem er bestimmte Richtlinien und Normen verfasst; das Bedürfnis nach der Sicherheit, die durch diese Regelwerke geschaffen werden soll, liegt aber letztendlich beim „Schutzbedürftigen", zum Beispiel dem Reisenden, selbst. Zur sicheren Gestaltung des Systems müssen also zunächst die „Schutzbedürftigen" identifiziert werden (siehe Abbildung 13).

Sobald die einzelnen „Schutzbedürftigen" identifiziert sind, müssen ihre sicherheitsrelevanten Anforderungen erfasst und strukturiert werden. Dies beinhaltet die Schwierigkeit, dass viele der sicherheitsrelevanten Anforderungen vom „Schutzbedürftigen" vorausgesetzt werden, er sich also nie bewusst vor Augen geführt hat, dass er diese Anforderungen hat. Dies erschwert die Erfassung der Anforderungen wesentlich. Bei der Strukturierung der Anforderungen muss zudem berücksichtigt werden, dass Sicherheit eine objektive, also messbare, Dimension und eine subjektive, von den einzelnen „Schutzbedürftigen" abhängige, Dimension hat. Beide Dimensionen können sich gegenseitig bedingen, müssen aber nicht zwangsläufig eine Wechselwirkung aufweisen.





Nachdem die Anforderungen auf aggregierter Ebene nach Anforderungen der objektiven und subjektiven Sicherheit strukturiert wurden, muss entschieden werden, welche der Anforderungen erfüllt werden müssen bzw. erfüllt werden sollen. Beispielsweise würde eine Anforderung an subjektive Sicherheit, die nur von einem sehr kleinen Personenkreis getragen wird, eventuell zugunsten einer breiter vertretenen Anforderung vernachlässigt. Eine weitere Möglichkeit zur Gewichtung der einzelnen Anforderungen ist die Betrachtung der mit ihnen verbundenen „Gefährder". Beispielsweise wird eine Anforderung, die mit einer gewollten Gefährdung in Verbindung gebracht werden kann, stärker berücksichtigt, selbst wenn es sich „nur" um eine Anforderung der subjektiven Sicherheit handelt.

Den umzusetzenden Anforderungen werden nun im 3. Schritt (siehe Abbildung 13) die nötigen „Schützer" gegenübergestellt.

Auf Basis dieser Planung kann nun mit der anforderungsgerechten Gestaltung des Systems Sicherheit begonnen werden. Dabei werden die auf Ebene des Gesamtsystems aggregierten Daten wieder den einzelnen Teilsystemen zugeordnet.





Abbildung 13: Anforderungsstrukturierung

Mitarbeiter ③
Unternehmen des Fahrgastes 1
Angehöriger
Angehöriger
Angehöriger
Fahrgast 1
Fahrgast 2
Fahrgast 3
Fahrgast n
①
Angehöriger
Schaffner
Zugführer
Bahnmitarbeiter y
Achse
Räder
Fenster
Sitze
Element x
ICE
Bauer an Bahnstrecke
Unternehmen „Bahn"
Wartungsmitarbeiter
Geschäftsführung
Angehöriger
Angehöriger
System „Einzugsbereich ICE" ②

1. Identifikation von Schutzbedürftigen

Schutzbedürftiger 1
Schutzbedürftiger 2
Schutzbedürftiger n

	SCHUTZBEDÜRFTIGER 1	SCHUTZBEDÜRFTIGER 2
OBJEKTIV	– technische Funktionsfähigkeit – Fahrtüchtigkeit – Zuverlässigkeit	– technische Funktionsfähigkeit – Fahrtüchtigkeit – Zuverlässigkeit
SUBJEKTIV	– solider optischer Eindruck – Sauberkeit	– Wachpersonal – Mitreisende gleichen Alters

2. Agregation der Anforderung in subjektive und objektive Sicherheitsanforderungen

3. Zuordnung der nötigen „Schützer" zu den Sicherheitsanforderungen

SCHÜTZER	ANFORDERUNGEN AN OBJEKTIVE SICHERHEIT				ANFORDERUNGEN AN SUBJEKTIVE SICHERHEIT			
	Fahrtüchtigkeit	technische Funktionsfähigkeit	Zuverlässigkeit	Zustände der Schienen	Wachpersonal	solider optischer Eindruck	Sauberkeit	Mitreisende
Schaffner 1	⊘	⊘	⊘	⊘	⊘	⊘	☺	☺
Schaffner 2	⊘	⊘	⊘	⊘	⊘	⊘	☺	☺
Wartungsmitarbeiter	☺	☺	☺	☺	⊘	☺	⊘	⊘
Reinigungskraft 1	⊘	⊘	⊘	⊘	⊘	☺	☺	⊘
Reinigungskraft 2	⊘	⊘	⊘	⊘	⊘	☺	☺	⊘
Zugführer	☺	☺	⊘	⊘	⊘	⊘	⊘	⊘
Konstrukteur	☺	☺	☺	⊘	⊘	⊘	⊘	⊘
Wachleute	⊘	⊘	⊘	⊘	☺	⊘	⊘	⊘

4. Systemgestaltung








2.5 ZUSAMMENFASSUNG

Die Entstehung des Produkts „Sicherheit" wurde anhand eines allgemeinen Systemmodells analysiert, das die Wechselbeziehung zwischen den drei Entitäten Schutzbedürftiger, Schützer und Gefährder allgemein beschreibt. Dieses Modell gilt unabhängig davon, ob die Gefährdung durch technisches oder menschliches Versagen (Safety), feindlichen Angriff (Security) oder Naturereignisse wie zum Beispiel Hochwasser hervorgerufen wird. Die Maßnahmen selbst, mit denen der Schützer den Schutzbedürftigen vor einer Schädigung durch den Gefährder bewahrt, unterscheiden sich aber in den Fällen gewollter und ungewollter Gefährdung. Bei der gewollten Gefährdung erfährt der Gefährder einen direkten Nutzen und wird seine Gefährdungsaktionen intelligent und mit Rücksicht auf die möglichen Schutzmaßnahmen planen. Der Schutzprozess oszilliert in diesem Fall, weil neue Gefährdungsmethoden neue Schutzmaßnahmen und diese wiederum neue Gefährdungsmethoden hervorrufen. Im Fall der ungewollten Gefährdung ist die Gefährdung Ergebnis eines stochastischen Prozesses, der mit statistischen Methoden beschrieben werden kann und damit eine Konvergenz des Schutzprozesses ermöglicht. Als wesentlich wurde erkannt, dass in allen Fällen der Schutzprozess nicht nur das Risiko mindern, sondern auch die Chancen bewahren, insgesamt also einen positiven Wert des Wagnisses erreichen muss, damit die Sicherheitsmaßnahmen dem Schutzbedürftigen nicht durch Einschnüren seiner Entfaltungsfreiheit mittelbar Schaden durch entgangenen Nutzen zufügen.




Auf Basis dieser Systemanalyse wurde der Generic Systems Engineering-Ansatz vorgestellt, der das vorhandene Potenzial des Systems Engineering zu einem ganzheitlichen Lösungsansatz ausbaut. Insbesondere wurden die Teilaspekte herausgegriffen, die sich mit der Schwierigkeit sowie den Konsequenzen einer Abgrenzung des betreffenden Systems befassen und die Strukturierung der sicherheitsrelevanten Anforderungen im und an das System betreffen. Diese Aspekte wurden anhand von Beispielen veranschaulicht. Im Ergebnis wurde deutlich, dass durch Systemanalyse und die Nutzung des Systems Engineering-Ansatzes der losen Sammelvokabel „Sicherheit" eine Struktur gegeben werden kann, die für die Gestaltung von Sicherheitsprozessen und den Entwurf von Sicherheitssystemen nützlich ist.

2.6 AUSBLICK

Mit dem hier vorgestellten Modellansatz ist ein Basisrahmen für die Analyse von Sicherheitsproblemen gegeben, der es erlaubt, auf systematische Weise nützliche Fragen zu stellen – nützlich im Hinblick auf die Gestaltung des schützenden Elements und damit der Maßnahmen, die dieses ergreift, um einen Sicherheitsbedarf zu befriedigen. Dieser Ansatz verlangt über den hier vorgestellten Umfang hinaus eine weitere Verfeinerung und Vertiefung der Schnittstellen zwischen den Systemelementen. Insbesondere ist die Wirkung des Gefährders auf den Schützer bisher noch ausgelassen. In diesem Fall





schlüpft der Schützer selbst in die Rolle des Schutzbedürftigen. Im Falle des Staates als Schützer schützt er alle seine Bürger. Damit sind auch Gefährder selbst wieder Schutzbedürftige. Diese Doppelrollen müssen in weiteren Modellierungsschritten berücksichtigt werden.

Als Basis für diese Betrachtung muss zunächst die Frage nach einer sinnvollen Systemgröße geklärt werden. Dabei ist nicht unbedingt eine Begrenzung ausschließlich anhand der Anzahl von Elementen sinnvoll (wobei diese natürlich im Hinblick auf die praktische Anwendbarkeit einer Systembeschreibung durchaus zu beachten ist). Vielmehr erscheint eher eine Betrachtung des Grades der Indirektheit, mit dem ein einzelner „Schutzbedürftiger" von einem Unglück oder einem anderen negativen Ereignis betroffen ist, sinnvoll.
Des Weiteren muss geklärt werden, ab welchem Stadium der Analyse davon ausgegangen werden kann, dass nun die relevanten Wechselbeziehungen zwischen den einzelnen Systemelementen bzw. Teilsystemen erfasst worden sind. Genügen an dieser Stelle eine bzw. mehrere „Expertenmeinungen" oder ist die Erarbeitung bestimmter Indikatoren notwendig?





Da nicht alle sicherheitsrelevanten Anforderungen in Regelwerken oder Gesetzen festgehalten sind, besteht im Rahmen der anforderungsgerechten Gestaltung des Systems Sicherheit außerdem Bedarf nach einer Entscheidungshilfe zur Auswahl der umzusetzenden Sicherheitsanforderungen. Hierbei spielen vor allem die Kategorisierung der einzelnen Anforderungen nach subjektiver und objektiver Sicherheit sowie die Gewichtung der Anforderungen eine wichtige Rolle. In diesem Zusammenhang stellt sich zudem die Frage nach der Erfassbarkeit insbesondere der Anforderungen, die die subjektive Sicherheit betreffen, sowie der Gewichtung dieser Anforderungen.

2.7 LITERATUR

Arlt 1999
Arlt, W.: Systemansatz eines produkt- und ablauforientierten Qualitätsmanagements durch Integration. Berlin: Systemtechnik, 1999.

Berger 1985
Berger, J. O.: Statistical Decision Theory and Bayesian Analysis, 2. Aufl. Heidelberg: Springer, 1985.

Beyerer 2009
Beyerer, J.: „Sicherheitstechnik, Sicherheitssysteme, und Sicherheitsforschung – Aktuelle Herausforderungen." In: Stober, R. (Hrsg.): Sicherheitsgewerbe und Sicherheitstechnik – Von der Personalisierung zur Technisierung – Ergebnisse des 9. Hamburger Sicherheitsgewerberechtstags. Köln, München: Carl Heymann, 2009, S. 1-10.





Der Spiegel 1998
Der Spiegel: Heimsuchung im High-Tech-Land. Der Spiegel (1998), Nr. 23, S. 22-34.

DIN 820-120
DIN Deutsches Institut für Normung e. V.: DIN 820-120: Normungsarbeit - Teil 120: Leitfaden für die Aufnahme von Sicherheitsaspekten in Normen. (ISO/IEC Guide 51:1999.) Berlin: Beuth, o. J.

DIN 2005
DIN Deutsches Institut für Normung e. V.: DIN-Fachbericht 144: Sicherheit, Vorsorge und Meidung in der Technik. Berlin: Beuth, 2005.

Haberfellner 1999
Haberfellner, R./Daenzer, W. F. (Hrsg.): Systems Engineering: Methodik und Praxis, 10. Aufl. Zürich: Verlag Industrielle Organisation, 1999.

Hollnagel et al. 2006
Hollnagel, E./Woods, D. D./Leveson, N. (Hrsg.): Resilience Engineering. Concepts and Precepts. Aldershot, England: Ashgate Publishing Limited, 2006.



Renn 2008
Renn, O.: Risk Governance. Coping with Uncertainty in a Complex World. London, England: Earthscan, 2008.

Renn/Walker 2008
Renn, O/Walker, K. (Hrsg.): Global Risk Governance. Concept and Practice Using the IRGC Framework. Doordrecht, Niederlande: Springer Verlag, 2008.

Renn et al. 2007
Renn, O/Schweizer, P.-J./Dreyer, M./Klinke, A.: RISIKO. Über den gesellschaftlichen Umgang mit Unsicherheit. München: oekom Verlag, 2007.

Sitte/Winzer 2004
Sitte, J./Winzer, P.: Systems Engineering: Old ideas, new potential. (2004 IEEE-SMC Konferenz.) Den Haag, Niederlande, 2004 – Tagungsband.





3 PRÄZISIERUNG DES NORMATIVEN SICHERHEITS-BEGRIFFS DURCH FORMALISIERTE BEGRIFFSBILDUNG

ECKEHARD SCHNEIDER/LARS SCHNEIDER

3.1 KURZFASSUNG

Der vorliegende Beitrag verfolgt das Ziel, auf der Grundlage eines interdisziplinären methodischen Ansatzes ein konsistentes Begriffsgebäude für den Begriff der Sicherheit zu entwerfen. Dies wird durch die integrative Verknüpfung zuvor terminologisch stringent formulierter und formalisierter Teilbegriffssysteme erreicht. Als Ergebnis dieser Vorgehensweise wird der Zusammenhang zwischen den elementaren Systemeigenschaften der Zuverlässigkeit und Instandhaltbarkeit und den emergenten Eigenschaften der Sicherheit und Verfügbarkeit in einer integrierten Darstellung formalisiert. Damit wird der komplexe Eigenschaftsbegriff der Sicherheit in seiner Binnenstruktur differenziert und durch geeignete Beziehungen konkretisiert sowie konsequent auf empirisch beobachtbare oder prognostizierbare Größen zurückgeführt.

3.2 ERFOLGREICHE KOMMUNIKATION ALS VORAUSSETZUNG FÜR SICHERHEIT

These 1: Wertschöpfung ist Kommunikation.

In der Sicherheitstechnik verursachen Kommunikationsprobleme infolge mangelhafter Begriffsbildung volkswirtschaftliche Verluste:

- *verschlechtertes Kosten-Nutzen-Verhältnis infolge erhöhter Fehlleistungskosten,*
- *Fehlgebrauch und Unfälle infolge fehlinterpretierter Normen, Spezifikationen und Gebrauchsanleitungen,*
- *fehlende Rechtssicherheit und Auslegungsprobleme bei mehrdeutigen Formulierungen in Verträgen und Rechtsvorschriften.*

Sicherheit als gesellschaftlicher Wert wird durch die Legislative in Regelwerken mit unterschiedlicher Detaillierung kodifiziert, deren Einhaltung die Organe der Judikative und Exekutive sicherstellen. Die technische Realisierung durch Sicherungstechnik und der gefahrlose Betrieb sind an zum Teil hochgradig ausdifferenzierte Regularien gebunden. Im Detail weisen derartige Begriffssysteme der Sicherheit jedoch Defizite auf. Diese müssen zur Erhöhung des Stands der Sicherheit behoben werden.





Gegenseitiges Verständnis aller Beteiligten verschiedener Disziplinen ist im gesamten Lebenslauf technischer Systeme entscheidend. Dazu gehören alle Phasen von der Systemkonzeption über die Entwicklung bis zum verlässlichen Betrieb. Die Entwicklung der zunehmend komplexen Systeme beginnt oftmals mit einer Formulierung der Anforderungen in natürlicher Sprache. Die auf diese Weise fixierten Anforderungen enthalten lexikologische Unschärfen.

Missverständnisse in der Kommunikation können Schäden hervorrufen, die neben dem Verlust des Vertrauens oder der physischen und psychischen Unversehrtheit erhebliche finanzielle Einbußen und weitere Schäden umfassen. Diese sind mehr oder weniger qualifizierbar und quantifizierbar. Es ist ein moralischer Anspruch und kultureller Wert, Schäden jedweder Natur zu vermeiden. Dieser gipfelt in dem Anspruch, Sicherheit zu entwickeln. Sicherheit erfordert daher fehlerfreie Kommunikation und somit ein allgemein übereinstimmendes Verständnis von Begriffen im Umgang mit technischen Systemen. Dazu dienen Normen im Sinne anerkannter Regeln der Technik. Diese enthalten sowohl Begriffsdefinitionen technischer Sachverhalte und technischer Prozesse im gesamten Lebenslauf als auch verbindliche Regeln für die Sprachproduktion und -rezeption als Mittel der Regelsetzung und ihres Verständnisses.



Technische Systeme können nur dann mit wirtschaftlichem Erfolg und der geforderten Sicherheit betrieben werden, wenn Kommunikation als Prozess der reziproken Bedeutungskonstruktion erfolgreich ist. Die Normung als Maßstab technisch einwandfreien Handelns berücksichtigt die Bedeutung einer präzisen Begriffsbildung für die Wirtschaftlichkeit und Sicherheit technischer Systeme bislang nur unzureichend. Sie ist vielmehr widersprüchlich und inkonsistent, was im nächsten Abschnitt gezeigt wird.

3.3 DEFIZITE DER AKTUELLEN BEGRIFFSBILDUNG DER SICHERHEIT IN TECHNISCHEN NORMEN

These 2: Feststellung

In der allgemein- und fachsprachlichen Kommunikation nimmt die Divergenz und Erosion im Begriffsfeld der Sicherheit und des Risikos zu:

- *Mehrdeutigkeiten durch exzessiven Gebrauch von Synonymen,*
- *begriffliche Unschärfe existierender Ausdrücke (Vagheit),*
- *Inkonsistenzen der Begriffssysteme (zum Beispiel Autohyponymien),*
- *Benennungsbildung ohne Begriffssystembezug,*
- *Inkompatibilität domänenspezifischer Glossare und*
- *drohender Domänenverlust der Deutschen Sprache.*





In vielen normativ verbindlichen Dokumenten sind die Termini der Sicherheit technischer Systeme zurzeit mehrdeutig und widersprüchlich festgelegt. Zur Untersuchung der gegenwärtig verwendeten Terminologie wurde ein Textkorpus aus einschlägigen nationalen und internationalen Normen und Richtlinien zusammengestellt. Auf dieser Grundlage wurden die bestehenden Defizite der Terminologie identifiziert und in These 2 benannt.[1]

Der Gegenstandsbereich der Sicherheit technischer Systeme ist gekennzeichnet von vielen synonym zueinander verwendeten Benennungen, wie Abbildung 1 zeigt. Dies führt zu Missverständnissen in der Zusammenarbeit von Beteiligten verschiedener Anwendungsdomänen. Ein erhöhter Abstimmungsaufwand und die damit verbundene Gefahr von Fehlleistungskosten erfordern daher eine terminologische Kontrolle. Diese zeigt sich unter anderem durch die konsequente Vermeidung von Mehrfachbenennungen.

Abbildung 1: Synonymie in der sprachlichen Repräsentation




BENENNUNG	DEFINITION
Gefährlicher Vorfall	Gefährungssituation, die zu einem Schaden führt
Schadensereignis	
Unfall	
Notfall	
unerwünschtes Ereignis	

Eine größere Stringenz in der Benennungsbildung abstrakter Begriffe kann mittels Integration zweier oder mehrerer formalisierter Modellkonzepte erreicht werden: Dies ist zum einen das Modellkonzept des Begriffs, welches die Differenzierung zwischen *Benennung* und *Definition* als unterschiedliche Ausprägungen der sprachlichen Repräsentation eines Begriffs vornimmt und weitere Eigenschaften unterscheidet. Zum anderen erlaubt das Modellkonzept des Systems eine Differenzierung hinsichtlich weiterer interessierender Modellaspekte.

Da die *Kausalität* und *Dynamik* von Systemen als Eigenschaften für die Klärung des Sicherheitsbegriffs als hilfreich und notwendig erachtet werden, liegt eine komplementäre Kategorisierung der außersprachlichen Bezugsobjekte in *Zustände* oder *Ereignisse* auf der Hand. Beide können in einem nächsten Schritt durch Größen und Werte

1 Schnieder 2009.





attributiert werden. Existiert darüber hinaus eine Nomenklatur im Sinne eines systematischen Satzes an Benennungsregeln, können zukünftig die aktuell bestehenden und hier in diesem Beitrag aufgezeigten Mehrdeutigkeiten und Widersprüche vermieden werden.

Abbildung 2 verdeutlicht beispielhaft derzeit bestehende logische Widersprüche in der Festlegung von Begriffen im Wortfeld der Sicherheit. Die sprachliche Fixierung von Begriffen erfolgt durch Benennungen und Definitionen. Im Konkreten sind sie äquivalente Instanziierungen der sprachlichen Repräsentation eines Begriffs.[2] Legt man der Analyse des terminologischen Bestands die Differenzierung zwischen Zuständen und Ereignissen zugrunde, so offenbaren sich hier logische Widersprüche. Der Wahrheitswert der Benennung wird durch die Interpretation der Definition in Frage gestellt. Für solche aus der Divergenz von Definition und Benennung beim Rezipienten resultierenden kognitiven Dissonanzen sind in Abbildung 2 verschiedene Beispiele aus dem Begriffsfeld der Sicherheit aufgeführt.

Abbildung 2: Kategorielle Widersprüche zwischen Benennung und Definition im Wortfeld der Sicherheit




			KATEGORIE DES AUSSERSPRACHLICHEN BEZUGSOBJEKTS	
QUELLE	KLASSE/KATEGORIE DER SPRACHLICHEN REPRÄSENTATION	INSTANZIIERUNG DER SPRACHLICHEN REPRÄSENTATION	ZUSTAND	EREIGNIS
[DIN EN 61508-4; 3.1.4]	Benennung	gefährlicher Vorfall		x
	Definition	Gefährdungssituation, die zu einem Unfall führt	x	
[IEC 61508-4; 3.1.4]	Benennung	hazardous event		x
	Definition	hazardous situation which results in harm	x	
[DIN V 19250; 2.8]	Benennung	unerwünschtes Ereignis		x
	Definition	Fehlzustand einer Betrachtungseinheit	x	

Eine bloße Kategorisierung der außersprachlichen Bezugsobjekte in Zustände und Ereignisse ist für eine eindeutige begriffliche Festlegung zwar notwendig, jedoch nicht hinreichend. Im Sinne einer eindeutigen Festlegung der Begriffe ist eine Klärung ih-

2 Vgl. DIN 2330.





res Kausalzusammenhangs zwingend. In der Normung ist dies oftmals nicht der Fall.[3] Liegt jedoch einem Sachverhalt in einer Norm eine Vorstellung über Kausalrelationen zugrunde, sind diese nicht zwangsläufig explizit ausgewiesen und somit für den Leser nicht eindeutig nachvollziehbar oder aber die identifizierten Kausalrelationen sind widersprüchlich (vgl. Abbildung 3).

Zum Begriff des Ausfalls als „Beendigung der Fähigkeit einer Funktionseinheit, eine geforderte Funktion auszuführen"[4] liegt hinsichtlich seiner Definition in der Normung ein Konsens vor: Der Ausfall wird übereinstimmend als Ereignis eingeordnet. Es besteht jedoch im Detail eine unterschiedliche Auffassung über die Einordnung des kausal mit dem Ausfall verbundenen Begriffs des Fehlers in das Begriffssystem der Verlässlichkeit technischer Systeme. Die unterschiedliche Auffassung des Fehlers als Vorbedingung (Ursache) oder Nachbedingung (Wirkung) des Ereignisses (hier: Ausfall) erschwert eine fehlerfreie Kommunikation oder macht diese gar unmöglich.




Abbildung 3: Kategorielle Widersprüche zwischen verschiedenen Begriffsdefinitionen

				ZUSTANDS-KATEGORIE	
QUELLE	BENENNUNG	DEFINITION	BEZUGS-BEGRIFF	VORBE-DIN-GUNG	NACH-BEDIN-GUNG
[DIN EN 61508-4; 3.1.4]	Fehler (en: fault)	Nicht normale Bedingung, die [einen Ausfall] verursachen kann	Ausfall	x	
[IEV 191-05-01]	Fehlzustand (en: fault)	Zustand einer Einheit, indem sie unfähig ist, eine geforderte Funktion zu erfüllen [...]			x

Die obigen Ausführungen verdeutlichen, dass der Aufbau eines konsistenten Begriffssystems als Voraussetzung eindeutiger Kommunikation für die Sicherheit technischer Systeme unerlässlich ist. Nur auf diese Weise ist innerhalb einer Sprache eine eindeutige Abgrenzung und konsistente Festlegung von Begriffen möglich. Hinsichtlich des Inhalts und Umfangs von Begriffen werden unterschiedliche Begriffsverständnisse in verschiedenen Sprachen offenbar. Im internationalen fachsprachlichen Kontext können so die Äquivalenzgrade von Benennungen bestimmt werden.

3 Hänsel 2008.
4 Vgl. IEC 60050-191 und DIN IEC 61508.





3.4 ZIELE KONSISTENTER BEGRIFFSSYSTEMBILDUNG

These 3: Zielsetzung

Die Festlegung eines konsistenten Begriffssystems der Sicherheit mit eineindeutiger Benennungszuordnung ist notwendig, um:

- *Fehlleistungskosten zu vermeiden,*
- *die technische Gestaltung und Argumentation zu optimieren,*
- *den Rechtsrahmen zu harmonisieren,*
- *Fehldimensionierungen zu verringern und*
- *die Verletzbarkeit von Systemen zu reduzieren.*

Komplexe Automatisierungssysteme werden in einem zunehmend globalisierten wirtschaftlichen, technischen und gesellschaftlichen Kontext entwickelt und betrieben. Dies erfordert aus wirtschaftlichen Gründen eine systematische Auseinandersetzung mit einer methodischen Entwicklung. Die natürliche Sprache ist hierbei das bevorzugte Medium der Kommunikation. Um dieser zentralen Rolle einer Fachsprache in der Entwicklung automatisierungstechnischer Systeme gerecht zu werden, muss diese den folgenden Zielen entsprechen:




- *terminologische Vollständigkeit:* Die bestehende Vielfalt der Terminologie muss in einem ersten Schritt zunächst einmal erfasst und dargestellt werden. Hieraus wird der akute Handlungsbedarf ersichtlich. Auf der Grundlage gemeinsamer Modellkonzepte können eine Vergleichbarkeit gewährleistet, etwaige Bedeutungsunterschiede offenbart oder terminologische Lücken identifiziert werden.
- *Disambiguität:* Die gegenwärtigen, durch die fehlende Eindeutigkeit der Terminologie entstehenden Probleme müssen durch eine terminologische Kontrolle und formale Verifikation gelöst werden. Für Begriffe sind bevorzugte Benennungen festzulegen und Synonyme gesondert auszuweisen.
- *Konsistenz:* Durch eine stringente Verwendung von Modellkonzepten sind bestehende Inkonsistenzen aufzuzeigen und widerspruchsfreie Terminologiegebäude zu entwerfen.
- *Nomenklatur:* Das metasprachliche Modell des Terminus wird als methodisches Instrumentarium für eine Benennungsbildung verwendet. Die Stellung einzelner Termini innerhalb des Terminologiegebäudes erlaubt die Bildung von Benennungsregeln. Falls notwendig, können somit sinnvolle und konsistente Neologismen eingeführt oder bestehende Benennungen ersetzt werden.
- *Terminologische Präzision:* An die Stelle bestehender Vagheiten terminologischer Festlegungen muss eine Verbindliche Klärung der Umfänge und Inhalte von Begriffen treten. Es ist an dieser Stelle eine Begriffsklärung bis auf die Ebene prognostizierbarer oder empirisch beobachtbarer Größen und Werte durchzuführen.





- *Mehrsprachigkeit:* Der Aufbau eines mehrsprachigen Begriffssystems setzt die Präzisierung der Begriffe voraus. Auf dieser Grundlage gelingt es, Begriffe hinsichtlich ihres Umfangs und ihrer Stellung innerhalb eines Terminologiegebäudes zu verorten und zu strukturieren. Dies erlaubt die Harmonisierung ihrer Benennungen und Definitionen. Probleme im internationalen fachsprachlichen Kontext werden somit vermieden.
- *Domänen-Integration:* Domänenspezifisch divergierende Begriffsverständnisse der Verlässlichkeit sowie der deskriptiven Statistik und Metrologie werden verdeutlicht und somit die methodische Grundlage für eine präzisere Kommunikation im Kontext interdisziplinärer Zusammenarbeit geschaffen.

Die in Abschnitt 3.3 dargestellten Defizite der Begriffsbildung verdeutlichen, dass ein grundlegend neuer Ansatz für die Begriffsbildung erforderlich ist. Ein Beispiel für solche hinsichtlich der genannten Aspekte stringenten Begriffssysteme ist neben den Systemen wissenschaftlicher Namen der Biologie, Mineralogie und Medizin das System systematischer Namen für chemische Verbindungen der International Union of Pure and Applied Chemistry (IUPAC). In den jüngeren Ingenieurwissenschaften existieren solche systematischen Ansätze der Terminologiebildung bislang nicht.




Das Erreichen der in diesem Kapitel dargestellten Ziele konsistenter Begriffssystembildung ist auf der Grundlage eines Modellkonzepts des Terminus und seiner Formalisierung möglich. Mit den miteinander verschränkten Modellkonzepten des Begriffs und des Systems, welche auf der Basis formaler Beschreibungsmittel (zum Beispiel der Klassendiagramme aus der Unified Modelling Language oder Petrinetze) dargestellt werden, liegt der methodische Ansatz vor. Dieser wird im folgenden Abschnitt detailliert vorgestellt.

3.5 METHODISCHER ANSATZ DURCH FORMALISIERTE BEGRIFFSSYSTEMBILDUNG

These 4: Methodischer Ansatz

Ein konsistentes Begriffssystem wird erreicht, wenn:

- *der Informationsgehalt abstrakter Begriffe durch ihre formalen und symbolischen Relationen erhöht wird,*
- *die sprachliche Vielfalt durch Formalisierung kritisch reflektiert wird,*
- *die Unschärfe einer natürlichsprachlichen Begriffsbeschreibung durch eine Einbettung in Modellkonzepte verringert wird und*
- *abstrakte Begriffe konsequent auf empirisch beobachtbare oder prognostizierbare Größen zurückgeführt werden.*





3.5.1 VORGEHENSWEISE DER FORMALISIERTEN BEGRIFFSBILDUNG

Eine grundlegende Vorgehensweise naturwissenschaftlicher Erkenntnisgewinnung ist die Entwicklung konsistenter Begriffsgebäude mit:

- einer stringenten *Terminologie* als Gesamtheit der Begriffe und ihrer Bezeichnungen in einem Fachgebiet,
- einer ordnenden *Taxonomie*, welche durch die über mehrere Ebenen konsequent beibehaltenen Strukturierungsmerkmale ein stringentes Begriffssystem erzeugt sowie
- einer *Nomenklatur* als vorab festgelegte Bildungsregeln für Benennungen, durch welche sich ein Terminus in den systematischen Zusammenhang einer Terminologie einordnet, und
- einer *Quantifizierung*, durch welche die (physikalischen) Zusammenhänge zwischen Begriffen durch die Angabe mathematischer Relationen offenbar werden.

Über die Festlegung systematischer Zusammenhänge zwischen Begriffen hinaus lässt sich eine weitergehende terminologische Präzisierung erreichen. Eine solche Begriffsexplikation endet in der Definition von Größen und zwischen ihnen bestehenden mathematischen Relationen in formaler Symbolsprache („quantitativer Begriff" im Sinne Carnaps).[5] Der Wahrheitsgehalt dieser logischen Modellkonstrukte kann empirisch bestätigt werden. Eine Falsifikation kann derartige Strukturen leicht beschädigen. Der methodische Ansatz der formalisierten Begriffsbildung ist in Abbildung 4 auf Seite 83 dargestellt.

- Die *Metakognition* schafft das Bewusstsein, in Begriffen zu denken. Diese Ansätze entstammen der Sprachphilosophie und der Linguistik und werden oftmals in Bezug zu dem von Ogden und Richards postulierten semiotischen Dreieck[6] diskutiert.
- Der zweite Schritt ist die *Formulierung* der abstrakten und generischen (metasprachlichen) Begriffsstruktur. Diese ist inhaltlich zweckfrei und damit sowohl bezüglich ihrer Inhalte als auch der Sprache invariant. Die Grundlagen hierfür sind in den klassischen Arbeiten Wüsters reflektiert[7] und in Terminologiegrundnormen[8] umgesetzt worden.
- Der dritte Schritt ist die *Formalisierung* dieser abstrakten und generischen (metasprachlichen) Begriffsstruktur, das heißt ihre Mathematisierung. Dabei werden die Begriffe als Mengenelemente und ihre Relationen im mathematischen Sinne aufgefasst. So kann das formalisierte Begriffssystem auch – unabhängig vom

---

5 Carnap 1959.
6 Ogden 1974.
7 Wüster 1978.
8 DIN 2330 und DIN 2342:2004.







Bedeutungsgehalt – auf logische Konsistenz geprüft werden (zum Beispiel beim Vorliegen der Begriffsrelation der Autohyponymie). Von entscheidender Bedeutung ist dafür die Wahl geeigneter Beschreibungsmittel, um verschiedene Begriffe und Relationstypen zu repräsentieren. Durch die Reduktion des Symbolvorrats erzwingen Beschreibungsmittel eine Erkenntnis über den zugrunde liegenden Gegenstandsbereich. Sie erleichtern darüber hinaus die Kommunikation der mit ihrer Hilfe repräsentierten metasprachlichen (später im Sinne der Objektsprache auch außersprachlichen) Inhalte (Kalküle operieren auf den Repräsentanten).[9]

- Im vierten Schritt erfolgt eine *Quantifizierung* und somit der Übergang von einer qualitativen Stufe der Begriffsbildung, die sich in einer natürlichsprachlichen Bezeichnung der Merkmalsausprägungen äußert, zu einer quantitativen Stufe der Begriffsbildung.[10] Auf der Basis verbindlich vereinbarter Abbildungsvorschriften gelingt durch die Attributhierarchie von Eigenschaft, Merkmal, Größe und Wert eine weitergehende Begriffsbildung.
- In einem vierten Schritt folgt die *Instanziierung* formalisierter (begrifflicher) Modellkonzepte. Ergänzend zu dem bislang erörterten Vorgehen der Metakognition, Formulierung und anschließenden Formalisierung *abstrakter* Begriffe, beispielsweise des Begriffs als solchem, sind für die Strukturierung des eigentlichen Gegenstandsbereichs der Sicherheit weitere, *konkretere* Begriffe hilfreich. Der Systembegriff kann zum Beispiel nach dem vorangehenden Konzept selbst als Begriff strukturiert werden. In einer weiteren Konkretisierung kann der Systembegriff dazu „materialisiert“ werden, beispielsweise für ein Verkehrssystem. Im Sinne der Objektorientierung wird dieser Schritt auch als „Instanziierung einer Klasse“ bezeichnet (konkreter und abstrakter Begriff). Es ergibt sich somit eine Struktur aufeinander aufbauender Instanziierungen, welche zu immer konkreteren Begriffen führt.
- In einem nächsten Schritt erfolgt gegebenenfalls die *Integration* verschiedener Begriffskonzepte. Dies berücksichtigt, dass bei komplexen Begriffen die sequenzielle Folge von Metakognition, Formulierung, Formalisierung und Instanziierung allein nicht hinreichend ist. Häufig werden Begriffe kontextuell entwickelt, verstanden und kommuniziert. Insofern muss neben dem einen Begriff oder Begriffssystem auch der Kontextbegriff oder sein Begriffssystem existieren. In den Kontext wird nun der erste Begriff eingebettet oder es werden in ihn beide Begriffe oder Begriffssysteme integriert oder verschränkt. Eine besondere Stabilität erreicht das Fusionsergebnis als komplexes und konkretes Begriffssystem auf der Basis des gemeinsamen abstrakten Begriffsverständnisses des Begriffs als solchem. Es wird verstärkt durch gemeinsame, auf der Grundlage dieses meta-



9 Schnieder 1999, Schnieder 2003 und van Schrick 2002.
10 Carnap 1959.





sprachlichen Begriffsmodells instanziierte Modellkonzepte wie zum Beispiel des Systems und darüber hinaus durch die gemeinsamen Beschreibungsmittel der verschiedenen Begriffssysteme. Diese ermöglichen eine Integration auf der Ebene der Formalisierung.[11]

- Verfügen die Begriffe bereits über eine formale Beschreibung, kann sich eine weitere Formalisierung im Sinne einer *Transformation* in eine Ontologiesprache anschließen. Ontologiesprachen stellen eine formale Beschreibung der Terminologie einer Wissensdomäne dar. Ontologiesprachen beziehen sich in aller Regel auf Begriffe (Klassen oder Entitäten), Eigenschaften und Merkmale von Begriffen (Attribute) und die zwischen ihnen bestehenden Relationen (Assoziationen) sowie zusätzliche Sprachmittel für Einschränkungen (Vorgaben von Kardinalitäten oder Wertebereichen).
- Das Methodenrepertoire der Informatik eröffnet die *Verifikation* der terminologischen Zusammenhänge. Als Beispiel gilt der aus der Sprachphilosophie heraus entwickelte Satz an Werkzeugen, der im Zusammenhang mit der Methode „OntoClean" geschaffen wurde. Hiermit können Ontologien auf ihre Korrektheit bezüglich einiger grundsätzlicher Eigenschaften der Abstraktionsbeziehung hin überprüft werden, die als *taxonomische Korrektheit* bezeichnet wird.[12] Der Schwerpunkt liegt hierbei auf der Konstruktion korrekter Taxonomien, welche das Gerüst einer komplexen Ontologie darstellen. Für eine folgende Integration ist das Vorhandensein korrekter Taxonomien eine notwendige Voraussetzung.



Die in Abbildung 4 skizzierte Treppe der Begriffskonzept- und -modellentwicklung präzisiert unscharfe und vage begriffliche Vorstellungen inhaltlich und bringt sie in einen konsistenten Zusammenhang.

[11] Schnieder 2003.
[12] Hänsel 2008.







Abbildung 4: Schematische Darstellung der formalisierten Begriffsbildung

Verifikationsansatz
Verifikation
verifiziertes Terminologiegebäude
integrierte formalisierte Modellkonzepte
Integrationskonzept
Integration
formalisierte Modellkonzepte
Modellkonzepte
Instanziierung
formalisiertes quantifiziertes Begriffsmodell
Metriken
Quantifizierung
formalisiertes Modell des Terminus
(formales) Beschreibungsmittel
Formalisierung
Benennung (sprachliche Repräsentation)
Syntax und Semantik natürlicher Sprachen
Formulierung
Idee des Terminus (mentale Repräsentaion)
Semiotisches Dreieck





kognitive Schemata
(Meta-)Kognition
Objekt (außersprachliche Repräsentation)
Informationsgehalt/ Formalisierungsgrad

3.5.2 FORMALISIERUNGSKONZEPT

Durch geeignete Beschreibungsmittel können bestimmte Aspekte des Begriffskonzepts dargestellt werden. Durch die Abbildung des Begriffskonzepts auf deren Symbolvorrat werden die Begriffe als solche semantisch und syntaktisch spezifiziert und dadurch präzisiert. Nachfolgend werden mit UML-Klassendiagrammen und Petrinetzen zwei geeignete Beschreibungsmittel eingeführt.

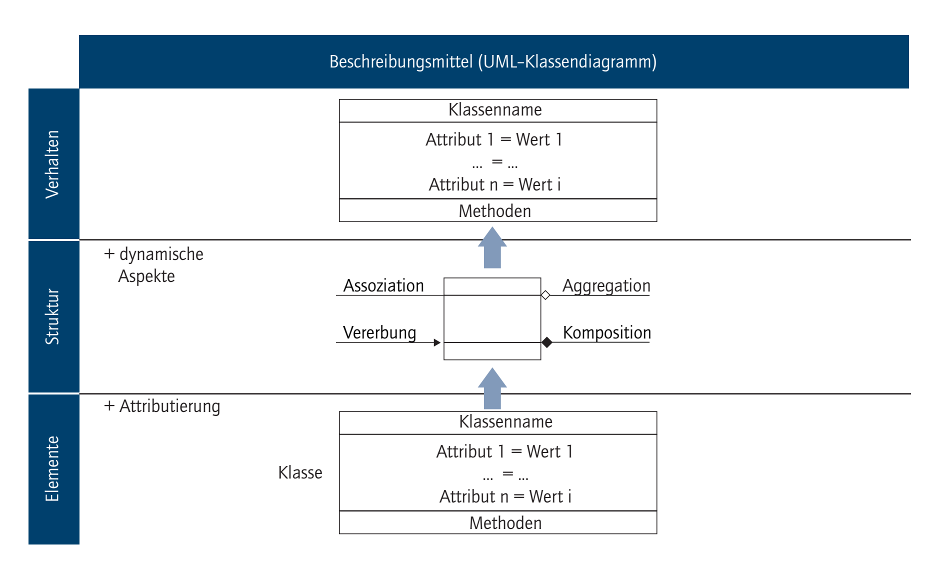




3.5.2.1 BESCHREIBUNG VON TERMINI MIT UML-KLASSENDIAGRAMMEN

Die Unified Modelling Language (UML) ist eine Sprache für die objektorientierte, grafische Darstellung des Aufbaus, des Verhaltens und der Funktionen von Systemen.[13] Im Folgenden wird der für diesen Beitrag wichtigste Diagrammtyp der UML, das Klassendiagramm, kurz vorgestellt. Klassendiagramme bilden den Kern der objektorientierten Modellierung und somit auch der UML. Dieser Diagrammtyp stellt vorwiegend die Systemstruktur dar, indem die Klassen und die zwischen ihnen bestehenden semantischen Beziehungen abgebildet werden (vgl. Abbildung 5).

Abbildung 5: Klassendiagramme als Beschreibungsmittel für Termini und ihre Nutzung zur Systembeschreibung und -modellierung





Eine „Klasse" ist in der Objektorientierung ein abstrakter Oberbegriff für die Beschreibung der gemeinsamen Struktur und des gemeinsamen Verhaltens von Objekten. Eine Klasse kann somit im vorliegenden Kontext betrachtet werden als „Denkeinheit, die aus einer Menge von Gegenständen unter Ermittlung der diesen Gegenständen gemeinsamen Eigenschaften mittels Abstraktion gebildet" wird.[14] Die Klasse ist somit einem Terminus gleichzusetzen.

- Jede Klasse hat einen *Namen*, als eine aus einem oder mehreren Wörtern bestehende Bezeichnung.

[13] Object Management Group 2009.
[14] DIN 2342:2004.





- *Attribute* spezifizieren die Objekte, die für diese Klasse gebildet werden. Attribute geben Eigenschaften und Merkmale von Klassen wieder, die zur Abgrenzung von anderen Klassen dienen.
- *Methoden* beschreiben die Aktionen, die Objekte jeder Klasse ausführen, und sind somit ein Ausdruck des Verhaltens eines Systems.

Mit der Identifizierung der Klassen werden auch die zwischen ihnen bestehenden Beziehungen spezifiziert, wodurch sich eine Systemstruktur definiert. In Klassendiagrammen können verschiedene semantische Relationen zwischen den Klassen dargestellt werden.

- Die *Vererbung* ist die Übergabe aller Attribute, Aktionen, Relationen und des dynamischen Verhaltens der Generalisierungsklasse an die Spezialisierungsklasse. Die Spezialisierungsklasse erweitert oder überschreibt eventuell die geerbten Eigenschaften.
- *Assoziationen* können nicht-hierarchische Begriffsbeziehungen darstellen, die auf thematischen Zusammenhängen beruhen. Sie können in Klassendiagrammen Zusammenhänge zu anderen Klassen herstellen oder auch auf sich selbst bezogen sein (reflexive Assoziation). In einer Assoziation kann auch eine *Kardinalität* angegeben werden, welche die Anzahl der assoziierenden Objekte jeder Klasse festlegt.




- Die *Komposition* verdeutlicht eine exklusive und existenzabhängige Beziehung zwischen dem Ganzen und seinen Teilobjekten. Auch hier kann die Anzahl der Objekte, die an einer exklusiven und existenzabhängigen Zugehörigkeitsrelation beteiligt sind, über Kardinalitäten festgelegt werden.
- Die *Aggregation* wird verwendet, um eine beliebige physikalische oder konzeptuelle Zugehörigkeit von Objekten einer Klasse zu Objekten einer anderen Klasse zu bezeichnen. Wie bei einer Assoziation kann auch hier eine Kardinalität angegeben werden.

3.5.2.2 BESCHREIBUNG VON TERMINI MIT PETRINETZEN

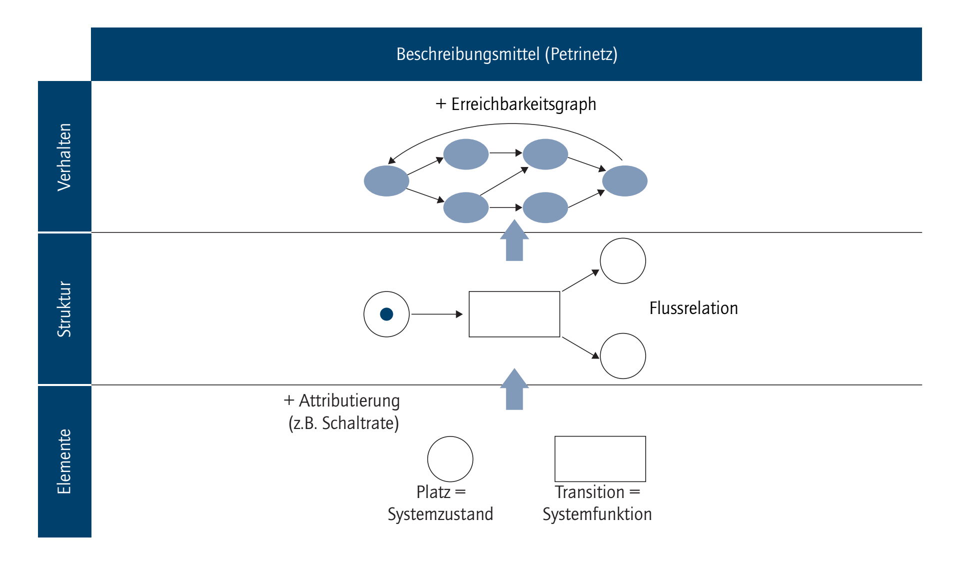
Das Beschreibungsmittel Klassendiagramm stellt die statische Struktur im Sinne der zwischen Klassen bestehenden Relationen geeignet dar. Zwar kann auch das Verhalten eines Objekts durch die Angabe von Methoden beschrieben werden, jedoch ist die Art der Darstellung nicht intuitiv. Diesen Nachteil der Klassendiagramme vermeiden prozedurale Beschreibungsmittel.





Zur *Formalisierung* terminologischer Zusammenhänge können die dynamischen (das heißt kausalen und temporalen) Begriffsbeziehungen beispielsweise mithilfe von Petrinetzen als Beschreibungsmittel widerspruchsfrei dargestellt werden.[15]

Abbildung 6: Petrinetze als Beschreibungsmittel für Termini und ihre Nutzung zur Systembeschreibung und -modellierung





Petrinetze bestehen, wie in Abbildung 6 dargestellt, aus den folgenden Elementen:

- *Plätze* können als Bedingungen, Voraussetzungen oder Zustände eines Systems interpretiert werden.
- *Transitionen* können als Ereignisse, Aktivitäten (Funktionen) oder Regeln eines Systems interpretiert werden.
- *Kanten* können als Kausalrelationen zwischen Plätzen und Transitionen interpretiert werden. Sie dienen der Darstellung der für ein System spezifischen Anordnung von Zuständen und Ereignissen. Gerichtete Kanten (Pfeile) zwischen Plätzen und Transitionen modellieren die logisch-dynamische Verknüpfung zwischen Zustandskombinationen als Bedingung für einen Zustandsübergang und den resultierenden Folgezuständen. Die Netztopologie beschreibt somit die kausale Struktur eines Systems und impliziert das Systemverhalten.



[15] Schnieder 1999, E DIN IEC 62551, VDI 4008, ISO/IEC 15909-1.





- *Marken* symbolisieren aktuell existente Zustände. Ist eine Bedingung zu einem Zeitpunkt erfüllt (lokaler Zustand), so ist der zugehörige Platz markiert. Die Menge der Marken aller zu einem Zeitpunkt erfüllten Bedingungen repräsentiert den globalen Zustand des diskreten Ereignissystems. Die Marken bewegen sich nach definierter Syntax und Semantik scheinbar in den Netzen, werden erzeugt und verschwinden. Durch den Markenfluss wird die Dynamik, das Verhalten des modellierten Systems unter den in der Struktur festgelegten Restriktionen, abgebildet.

Die zuvor genannten Grundelemente von Petrinetzen können attributiert werden, was eine Erweiterung der Mächtigkeit der Modellierung wiedergibt.

- *Temporale Attributierung der Netzelemente:* Zeitliche Vorgänge und Abhängigkeiten (Temporalität) können durch deterministisch oder stochastisch zeitbewertete Petrinetze geeignet beschrieben werden. Die Zeitbewertung erfolgt durch die Zuordnung von Zeitattributen zu den verschiedenen Strukturelementen eines Petrinetzes. Es ist somit möglich, Zeitattribute Kanten, Transitionen und Plätzen zuzuordnen.
- *Attributierung der Marken:* In höheren Petrinetzen ist es möglich, statt der zuvor anonymen Marken unterscheidbare und inviduelle Marken zu erzeugen. Eine Marke kann verschiedene Attribute aufweisen. Eine Stelle kann beliebig viele solcher komplexen Marken enthalten, die von den angeschlossenen Transitionen auf individuelle Weise verarbeitet werden können.




Die Struktur des Petrinetzes und die vorgenommenen Attributierungen sind impliziter Ausdruck des Systemverhaltens. Ausgehend von einer definierten Anfangsmarkierung kommt man durch das Schalten einer Transition zur nächsten Folgemarkierung des Petrinetzes. Der Erreichbarkeitsgraph ist die Menge aller von einer Anfangsmarkierung eines Petrinetzes aus erreichbaren Markierungen und schaltbaren Transitionen. Er veranschaulicht somit explizit die vollständige Dynamik des Petrinetzes.

3.5.2.3 KOMPLEMENTÄRE INTEGRATION AUF BESCHREIBUNGSMITTELEBENE

In den Ausführungen zur Formalisierung durch Beschreibungsmittel ist deutlich geworden, dass die semantische Mächtigkeit für die Qualität einer Begriffsfestlegung maßgeblich ist. Die Klassendiagramme der UML und die Petrinetze ergänzen sich gegenseitig hinsichtlich ihrer semantischen Ausdrucksstärke, da sie die zuvor dargestellten statischen und dynamischen Aspekte des Begriffs als solchem in einer integrierten Darstellung zusammenfassen.





- *Petrinetze ergänzen UML-Klassendiagramme* um die dynamischen Zusammenhänge technischer Systeme, da in ihnen die semantischen Aspekte der Kausalität und Temporalität darstellbar sind. Die die Dynamik eines Systems konstituierenden kausalen und temporalen Merkmale können selbst als Begriffe aufgefasst werden, was den Übergang zur zweiten Darstellungsform der UML-Klassendiagramme nahelegt.
- *UML-Klassendiagramme ergänzen die verhaltensorientierte Semantik von Petrinetzen* um Aspekte der statischen (Begriffs-) Systemstruktur. Die mit Petrinetzen kausal (im Sinne einer Halbordnung) verknüpften Geschehnis- oder Prozessbegriffe werden durch Klassendiagramme mittels der in Abschnitt 3.5.3.1 vorgestellten hierarchischen Struktur der Attribute ihrer Eigenschaften, Merkmale, Größen und Werte detailliert und verbindlich festgelegt. Die Definition eines Begriffs endet somit in der Definition von Größen und zwischen ihnen bestehenden mathematischen Relationen („quantitativer Begriff" im Sinne Carnaps).[16]

Abbildung 7 zeigt die integrierte Darstellung der statischen und dynamischen Aspekte von Begriffen. Die beiden Beschreibungsmittel entsprechen einander wie folgt:




- Der *Transition* eines Petrinetzes inklusive seiner zugehörigen Pre- und Postkanten (als Ausdruck ihrer Einbettung in die dynamische Systemstruktur) entspricht die *gerichtete Assoziation* in der Darstellung der UML-Klassendiagramme. In Analogie zu den gerichteten Kanten eines Petrinetzes ist sie nur in einer Richtung navigierbar. Der Assoziationsrelation ist eine Assoziationsklasse zugeordnet.
- Den *Plätzen* eines Petrinetzes entsprechen die *Klassen* der UML-Klassendiagramme.
- Die Möglichkeit der temporalen und stochastischen Attributierung von Petrinetzen korrespondiert mit der Angabe von Attributen für die (Assoziations-) Klassen von UML-Klassendiagrammen.

Die in diesem Abschnitt vorgestellte generische Schablone eines (formalisierten) Systemausschnitts wird in den folgenden Kapiteln durch geeignete konkrete Termini der Zuverlässigkeit und der Instandhaltbarkeit in jeweiligen Teilnetzen instanziiert und über Zustände als Fusionsplätze integriert.

---

[16] Carnap 1959.





Abbildung 7: komplementäre Integration auf Beschreibungsmittelebene




3.5.3 DAS METASPRACHLICHE MODELL DES TERMINUS UND SEINE FORMALISIERUNG

3.5.3.1 KONSTITUENTEN DES METASPRACHLICHEN MODELLS DES TERMINUS

In der terminologischen Grundnormung wird als „Terminus" das zusammenhängende Paar aus einem Begriff und seiner Benennung als Element einer Terminologie aufgefasst.[17] Ein Terminus ist somit ein „sprachliches Zeichen".[18] Aus der Sicht der linguistischen Zeichentheorie sind die menschliche Sprache und somit auch der Fachwortschatz ein komplexes Zeichensystem.[19] Mit dem Modell des sprachlichen Zeichens existiert in der Linguistik eine Vorstellung darüber, was die Natur von Wörtern ausmacht.[20] Die Zeichenauffassungen haben sich im Verlaufe des wissenschaftlichen Diskurses in der Semiotik grundlegend gewandelt.[21] Im vorliegenden Beitrag wird das bilaterale Zeichenmodell der terminologischen Grundnormung zu einem trilateralen Zeichenmodell erweitert.[22]

17 DIN 2342:2004.
18 Löbner 2002.
19 Keller 1995.
20 Kortmann 1999.
21 Keller 1995.
22 Vgl. auch Schnieder 2009.





Nach der ersten Übersicht werden die Konstituenten des metasprachlichen Modells des Terminus (vgl. Abbildung 8) im weiteren Verlauf dieses Kapitels detaillierter erläutert. Das metasprachliche Modell des Terminus umfasst die folgenden Konstituenten:

- eine *Bezeichnung* (Signifikant): Seine Repräsentation mit sprachlichen (Benennung) oder anderen Mitteln (Symbol, Formel). Aus Sicht der Lexikographie und Lexikologie wird der Signifikant[23] oder die Benennung[24] auch als „Lemma" bezeichnet.[25]
- den eigentlichen *„Begriff"* (Signifikat): Begriffe werden nach der DIN-Norm DIN 2342:2004 definiert als „Denkeinheit, die aus einer Menge von Gegenständen unter Ermittlung der diesen Gegenständen gemeinsamen Eigenschaften mittels Abstraktion gebildet wird." Begriffe dienen dem Erkennen von Gegenständen, der Verständigung über Gegenstände sowie dem gedanklichen Ordnen von Gegenständen.[26]
- eine *Varietät*, welche einen Rückschluss auf den Verwendungskontext eines sprachlichen Zeichens erlaubt.



Der eigentliche Begriff (Signifikat) lässt sich gemäß van Schrick[27] und DIN 2342:2004 weiterhin differenzieren in die folgenden Konstituenten:

- einen *Umfang* (Extension) als die Menge aller Gegenstände, die unter einen Begriff subsumiert werden,
- einen *Inhalt* (Intension) als die Eigenschaften eines Begriffs und die für ihn charakteristischen Merkmale mit ihren Größen (in Zahlen ausdrückbare Eigenschaften von Gegenständen) und Werten. Die Gesamtheit der wesentlichen Eigenschaften eines Gegenstands ist seine Beschaffenheit, die zeitlich veränderlich sein kann. Die zu einem bestimmten Zeitpunkt vorliegende Beschaffenheit ist der Zustand des betrachteten Objekts.[28]
- eine *Beziehung* (Relation) zu anderen Begriffen, welche aufgrund von Merkmalen besteht oder hergestellt wird. Die Relationen sind zentral, da der Begriff seine Bedeutung über die Stellung im System durch eine differenzlogische Bestimmung der Bedeutung erhält.
- eine *Definition*: Seine Begriffsbestimmung mit sprachlichen Mitteln. Diese Definition setzt eine Kenntnis des Umfangs, des Inhalts, der Relationen und des Bedeutungskontexts des Begriffs voraus.

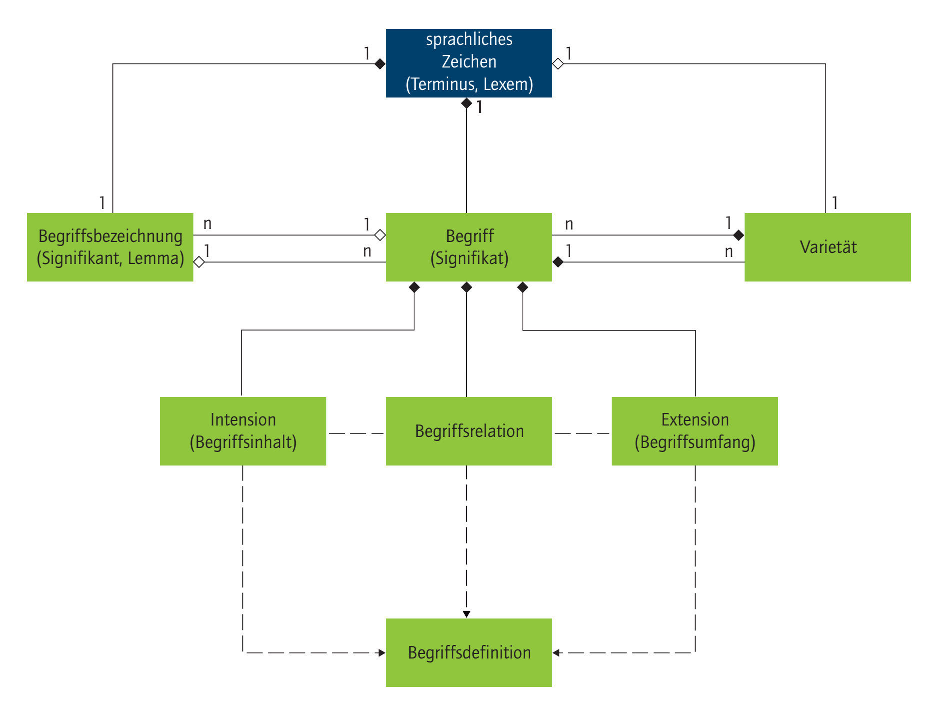
---

23 de Saussure 2001.
24 DIN 2342:2004.
25 Lutzeier 2007, Wolski 1989.
26 Arntz/Picht/Mayer 2004.
27 van Schrick 2002.
28 van Schrick 2002.





Abbildung 8: Konstituenten des metasprachlichen Modells des Terminus






Diese Konstituenten eines Terminus sind selbst wiederum sprachliche Zeichen. Eine formalisierte Darstellung dieses komplexen Sachverhalts zeigt Abbildung 8 in Form eines Klassendiagramms. In dieser Sicht wird der Terminus als eigenständiges metasprachliches Modell etabliert. Dieses Konzept ist hochgradig rekursiv, da die vorgestellten Konstituenten selbst wieder als sprachliche Zeichen aufgefasst werden müssen; dies ist in Abbildung 8 nicht dargestellt, um die Darstellung nicht zu überfrachten.

3.5.3.2 INHALT (INTEGRATION VERSCHIEDENER GRUNDNORMEN)

In Abbildung 9 ist der formalisierte „Begriffs"-Begriff in Form eines UML-Klassendiagramms vereinfacht dargestellt. Der Begriffsinhalt wird darin durch eine hierarchische Dekomposition der Attribute definiert.





Abbildung 9.1: Der Begriffsinhalt – formalisiert als UML-Klassendiagramm

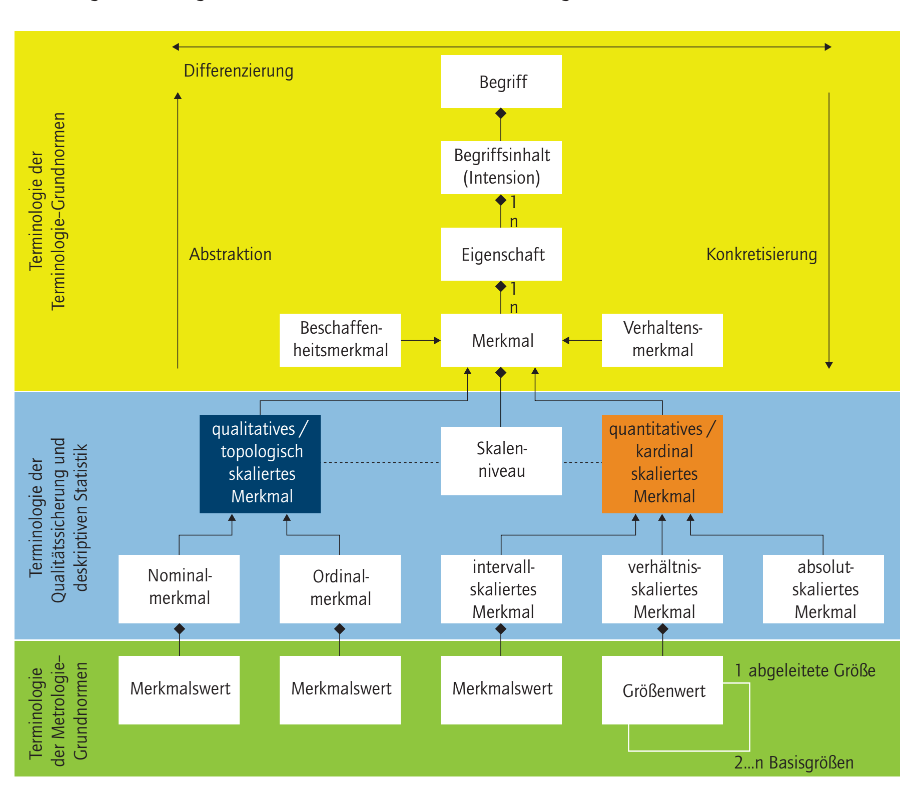


Abbildung 9.2: Detaillierung qualitativer/topologisch skalierter Merkmale

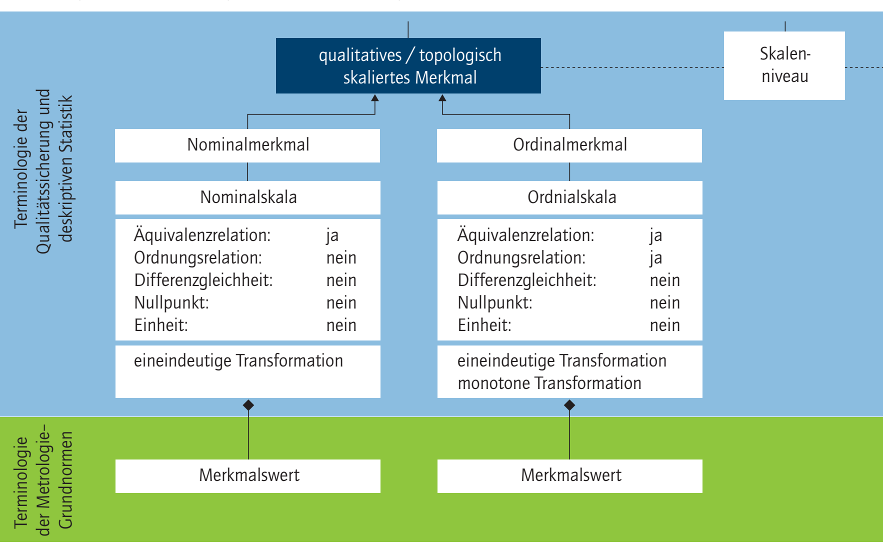








Abbildung 9.3: Beschriftung einfügen: Detaillierung quantitativer/kardinal skalierter Merkmale

Terminologie der Qualitätssicherung und deskriptiven Statistik

Skalenniveau

quantitatives / kardinal skaliertes Merkmal

diskretes Merkmal

kontinuierliches Merkmal

intervallskaliertes Merkmal

verhältnisskaliertes Merkmal

absolutskaliertes Merkmal

Intervallskala	Verhältnisskala	Absolutskala
Äquivalenzrelation: ja Ordnungsrelation: ja Differenzgleichheit: ja Nullpunkt: ja (willkürlich) Einheit: ja (willkürlich)	Äquivalenzrelation: ja Ordnungsrelation: ja Differenzgleichheit: ja Nullpunkt: ja (absolut) Einheit: ja (willkürlich)	Äquivalenzrelation: ja Ordnungsrelation: ja Differenzgleichheit: ja Nullpunkt: ja (absolut) Einheit: ja (natürlich)
eineindeutige Transformation monotone Transformation lineare Transformation Addition und Subtraktion	eineindeutige Transformation monotone Transformation lineare Transformation Addition und Subtraktion Multiplikation und Division	eineindeutige Transformation monotone Transformation lineare Transformation Addition und Subtraktion Multiplikation

Terminologie der Metrologie-Grundnormen

Merkmalswert

Größenwert

1 abgeleitete Größe

2...n Basisgrößen

Referenzwert

Koordinate (Differenzgröße)

Zahlenwert

Maßeinheit

1 abgeleitete Größe

2...n Basisgrößen

Zeichen

Vorsatzzeichen (Prefix)

Einheitenzeichen



– *Eigenschaften* beziehen sich auf eine potenziell wahrnehmbare Zustandsform der Wirklichkeit. Eigenschaften können mit Benennungen versprachlicht werden und stellen somit wieder Termini im Sinne der zuvor dargestellten Rekursivität des metasprachlichen Modells dar. Für eine Begriffsexplikation sind die Eigenschaften zu operationalisieren und somit auf empirisch beobachtbare Merkmale zurückzuführen. Den Eigenschaften von Gegenständen werden somit im Erkenntnisakt Merkmalsbegriffe zugeordnet.[29] Eigenschaften entstehen durch eine Abstraktion von den Merkmalen, beziehungsweise Eigenschaften werden durch eine Menge von Eigenschaften gekennzeichnet.

[29] Felber/Budin 1989.





- *Merkmalsbegriffe* sind Grundelemente für das Erkennen und Beschreiben von Gegenständen und das Ordnen von Begriffen. Merkmale sind objektiv bestimmbar und somit in objektiver Weise präzisierte Eigenschaften, durch die Objekten der außersprachlichen Wirklichkeit, die Träger der Merkmale sind, jeweils ein Merkmal als Kennzeichen der Erscheinungsform zugeordnet wird.[30] Ein Objekt kann Merkmalswerte unterschiedlicher Merkmale aufweisen, aber von jedem Merkmal kommt ihm nur ein Merkmalswert zu. Diese Merkmalswerte müssen für den jeweiligen Zweck hinreichend präzise festgelegt sein. Es muss somit ein prinzipielles Verfahren (beispielsweise Zählen oder Messen) geben, die Merkmalswerte für einen gegebenen Merkmalsträger zu ermitteln. Dies ist in der Regel die Vorgabe einer Systematik von Merkmalswerten (Skalenniveau), aus der hervorgeht, wie sich der Merkmalswert einordnet.[31] Merkmale sind demnach einer Messung (kontinuierliche Merkmale) oder Zählung (diskrete Merkmale) zugänglich. Merkmale sind selbst Begriffe.[32]
- Der *Größenbegriff* ist ein Spezialfall des allgemeineren Merkmalsbegriffs. Größenbegriffe in der Physik beziehen sich auf eine Klasse von Klassen physikalischer Phänomene – oder auf eine Klasse physikalischer Eigenschaften, die eine Skala numerischer Messwerte ausmachen und die man konkreten Phänomenen zusprechen kann, die sich unter wohl definierten experimentellen Bedingungen erzeugen lassen. Die Festlegung einer physikalischen Größe beinhaltet neben der topologischen Definition (Äquivalenz- und Ordnungsrelation) auch die metrische Definition (Festlegungen zu Skalenform, Nullpunkt und Einheit).[33] Nach deutschem Verständnis beschränkt sich somit der Begriff „Größe" auf verhältnisskalierte Merkmale, sodass es keine Ordinalgrößen, sondern nur Ordinalmerkmale gibt. Eine so definierte Größe ist Bestandteil eines Größensystems als einer Menge von Größen und einer Menge widerspruchsfreier Gleichungen, die diese Größen zueinander in Beziehung setzen. Durch diese Einbettung einer einzelnen Größe in ein Größensystem ergibt sich die Differenzierung des Oberbegriffs „Größe" in die Unterbegriffe der Basisgrößen und abgeleiteten Größen.[34] Dies ist im UML-Klassendiagramm (vgl. Abbildung 9) als reflexive Assoziation dargestellt.
- Jeder spezielle *Wert* einer Größe (Größenwert) kann als Produkt aus Zahlenwert und Maßeinheit dargestellt werden. Die Maßeinheit ist hierbei ein durch internationale Übereinkunft definierter reeller skalarer Wert, mit dem jeder andere Wert der Größe verglichen und als Verhältnis der beiden Größenwerte als Zahlenwert




[30] DIN 1313.
[31] DIN 1313.
[32] Felber/Budin 1989.
[33] Carnap 1959.
[34] ISO/IEC Guide 99.





ausgedrückt werden kann. Analog zur Größe kann auch bei den Einheiten zwischen „Basiseinheiten" (Meter als Basiseinheit der Größe Länge) und „abgeleitete Einheiten" (Meter durch Sekunde als abgeleitete Einheit der abgeleiteten Größe Geschwindigkeit) unterschieden werden.[35]

3.6 DER SICHERHEITSBEGRIFF ALS FORMALISIERTES BEGRIFFSSYSTEM

These 5: Explikation des Sicherheitsbegriffs

Ein präzises Begriffssystem des Sicherheitsbegriffs wird erreicht, wenn:

- *das Modellkonzept des Systems mit grundlegenden und emergenten Eigenschaften sowie mit den zwischen ihnen bestehenden Emergenzrelationen (Systemstruktur) durch geeignete Beschreibungsmittel formalisiert wird,*
- *die Begriffe der Zuverlässigkeit und Instandhaltbarkeit als elementare Eigenschaften eines konkreten Systems aufgefasst werden,*
- *der abstrakte Begriff der Sicherheit als emergente Eigenschaft eines konkreten Systems aufgefasst wird,*
- *sämtliche Eigenschaftsbegriffe auf empirisch beobachtbare oder prognostizierbare Größen zurückgeführt und quantifiziert und die zwischen ihnen bestehenden mathematischen Zusammenhänge infolge der Emergenzrelation (Systemstruktur) formal gefasst werden.*

In diesem Abschnitt wird für den Sicherheitsbegriff ein formales Begriffssystem entwickelt. Hierzu werden zunächst die diesen Begriff konstituierenden Teilbegriffe der Zuverlässigkeit und Instandhaltbarkeit gemäß der in Abschnitt 3.5.3.3 geschilderten Vorgehensweise strukturiert. Der strukturelle Isomorphismus, welcher sich in dem gemeinsam zugrunde gelegten Begriffsmodellkonzept und den formalen Beschreibungsmitteln äußert, erlaubt die Integration zu einem formalen Begriffssystem des Sicherheitsbegriffs. Dieses Begriffssystem erstreckt sich bis auf die Ebene konkret beobachtbarer und prognostizierbarer Größen.

Sobald sich ein offenes und komplexes System durch Kombination seiner Teile bildet, entstehen in der Realität durch die Wechselwirkungen Eigenschaften, die zuvor nicht beobachtbar waren und die auch nicht aus den Eigenschaften ihrer bislang isolierten Teilsysteme heraus erklärbar sind.[36] Dieses Phänomen bezeichnet die Systemtheorie als „Emergenz".[37] Nach Schnieder[38] können die Eigenschaften technischer Systeme in „elementare" und „emergente Eigenschaften" unterschieden werden:

---

[35] ISO/IEC Guide 99.
[36] Vester 2002.
[37] von Bertalanffy 1969, Willke 2000.
[38] Schnieder 2009.







- *Elementare Eigenschaftsbegriffe* eines Systems sind sein Zustand im Sinne der zu einem gegebenen Zeitpunkt vorhandenen physikalischen und informatorischen Eigenschaften, Merkmale, Größen und Werte sowie seine Funktion im Sinne einer Abbildungsvorschrift, welche Zustandsmengen der Eingangsgrößen in Zustandsmengen der Ausgangsgrößen überführt. Für eine gegebene Komponente sind der nicht erkannte Fehlzustand und der funktionsfähige Zustand solche elementaren Eigenschaften. Die Zuständsübergänge zwischen diesen elementaren Zuständen ist der Ausfall (vgl. Zuverlässigkeit) und die Wiederherstellung (vgl. Instandhaltbarkeit).
- *Emergente Eigenschaftsbegriffe* bezeichnen Systemeigenschaften, insbesondere Verhaltensweisen, die neu und charakteristisch für das Gesamtsystem sind. Diese Eigenschaften sind nicht den Elementen zuzurechnen, sondern resultieren aus der bestimmten selektiven Verknüpfung (Struktur) der Komponenten des Systems.[39]

So ist die Sicherheit eine emergente (Verhaltens-) Eigenschaft. Sie kann durch Struktur- und Parametervariation beeinflusst werden.



- Die *Parametervariation* bedeutet, dass gezielt die elementaren Eigenschaften technischer Systeme (zum Beispiel Bauteileigenschaften im Sinne der Überlebenswahrscheinlichkeit) beeinflusst werden. Erst im Kontext des Gesamtsystems werden diese zu einer höheren Sicherheit führen.
- Die *Strukturvariation* bedeutet, dass gezielt mehrkanalige Aufbaustrukturen realisiert werden, um auch im Falle des Funktionsversagens einer Einheit die Sicherheit aufrecht zu erhalten. In einem anderen Sinne stellt auch die Funktionsverknüpfung im Sinne geschlossener (rückgekoppelter) Wirkungsabläufe eine Maßnahme der Strukturvariation dar.



Struktur und elementare Eigenschaften sind somit mögliche Maßnahmen, das Verhalten (die Sicherheit) auf der Ebene des Gesamtsystems zu beeinflussen.

[39] Willke 2000.





3.6.1 ELEMENTARE EIGENSCHAFTEN

3.6.1.1 INSTANZIIERUNG DES ZUVERLÄSSIGKEITSBEGRIFFS

Unter der „Zuverlässigkeit“ wird die Fähigkeit einer Einheit verstanden, eine geforderte Funktion unter gegebenen Bedingungen für ein bestimmtes Zeitintervall zu erfüllen.[40] Für die Begriffsklärung der „Zuverlässigkeit“ sind vereinfachend zwei komplementäre Zustände notwendig:

- Die Funktionsfähigkeit ist die Fähigkeit einer Einheit, eine geforderte Funktion unter gegebenen Bedingungen für ein bestimmtes Zeitintervall zu erfüllen.[41] Diese wird einem Zustand zugeordnet, der im Folgenden als *funktionsfähiger Zustand* bezeichnet wird.
- Unter einem *Fehlzustand* wird der Zustand einer Einheit verstanden, in dem sie unfähig ist, eine geforderte Funktion zu erfüllen. Wenn ein funktionsunfähiger Zustand durch Wartung oder andere geplante Handlungen verursacht wird oder durch das Fehlen äußerer Mittel hervorgerufen wurde, wird er hierbei explizit nicht als Fehlzustand angesehen. Wird der Fehlzustand als wahrscheinlich eingestuft, Personenschäden, Sachschäden oder andere unvertretbare Schäden zu verursachen, spricht man von einem *kritischen Fehlzustand.*[42]





Der *Ausfall* ist die Beendigung der Funktionsfähigkeit einer Einheit. Dieses Ereignis stellt den Zustandsübergang zwischen dem funktionsfähigen Zustand und dem Fehlzustand dar. Hat der Ausfall einen kritischen Fehlzustand zur Folge, handelt es sich um einen kritischen Ausfall.

Der Ausfall ist ein nicht determinierbares Ereignis, da sein tatsächlicher Zeitpunkt in der Regel nicht exakt bestimmt werden kann. Mithilfe der Wahrscheinlichkeitstheorie und deren aggregiertem Maß der Wahrscheinlichkeit ist es möglich, global quantitative Aussagen über nicht determinierbare Ereignisse zu treffen.[43] Es ist hierbei das Ziel, die charakterisierenden Eigenschaften des Systems durch Zuverlässigkeitskenngrößen statistisch zu quantifizieren. Die Zeitspannen, die mit den Eigenschaften einer Betrachtungseinheit verbunden sind, werden in der Zuverlässigkeit durch Zufallsvariablen beschrieben. Den Zufallsvariablen werden Wahrscheinlichkeitsfunktionen zugeordnet.

---

40 VDI 4001.
41 IEC 60050-191.
42 IEC 60050-191.
43 Rakowsky 2002.





- Die Dauer des *funktionsfähigen Zustands* als seine Größe ist eine Zufallsvariable. Dieser Zustand besteht für eine gewisse Zeit. Es ergibt sich somit eine Überlebenswahrscheinlichkeit als Merkmal, dass eine Einheit eine geforderte Funktion für ein gegebenes Zeitintervall erfüllen kann.[44] Diese Wahrscheinlichkeitsfunktion kann durch die Überlebenswahrscheinlichkeitsverteilungsfunktion R(t) beschrieben werden.
- Der *Fehlzustand* ist komplementär zum funktionsfähigen Zustand und hat ebenfalls eine zufallsverteilte Dauer. Es ergibt sich somit eine Ausfallwahrscheinlichkeit als Merkmal, dass eine Einheit eine geforderte Funktion für ein gegebenes Zeitintervall nicht erfüllen kann.[45] Da es sich um gegensätzliche Zustände handelt, sind auch die Wahrscheinlichkeiten komplementär. Die *Ausfallwahrscheinlichkeitsverteilungsfunktion* F(t) ist somit das Komplement der Überlebenswahrscheinlichkeitsverteilungsfunktion R(t) zum Zahlenwert eins.
- Die zeitliche Änderung der Ausfallwahrscheinlichkeit ist die *Ausfallwahrscheinlichkeitsdichtefunktion*.[46] Sie berechnet sich als erste Ableitung aus der Ausfallwahrscheinlichkeitsverteilungsfunktion oder der negativ bezifferten Überlebenswahrscheinlichkeitsverteilungsfunktion.




Der Erwartungswert der Überlebenswahrscheinlichkeitsdichtefunktion stellt ein Maß für die zu erwartende Dauer bis zur Beendigung der Funktionsfähigkeit dar. Dieser Wert wird als *mittlere Dauer bis zum Ausfall* bezeichnet (englisch: „mean time to failure", MTTF). Die Dauer bis zum Ausfall ist die akkumulierte Dauer der Betriebszeit einer Einheit ab Nutzungsbeginn bis zum Ausfall oder ab dem Zeitpunkt der Wiederherstellung bis zum nächsten Ausfall.

Eine weitere wichtige Kenngröße, welche die verschiedenen Überlebenswahrscheinlichkeitsverteilungen charakterisiert, ist die *Ausfallrate*. Die Ausfallrate $\lambda(t)$ ist die relative zeitliche Änderung der Ausfallwahrscheinlichkeit, indem diese auf die Überlebenswahrscheinlichkeit bezogen wird.[47]

Aus den zuvor genannten Zuverlässigkeitskenngrößen lassen sich die notwendigen Kenngrößen für eine Sicherheitsbetrachtung ableiten. Allerdings werden hier nicht alle berücksichtigt, sondern die sicherheitsrelevanten Teilmengen dieser Ereignisse (kritischer Ausfall), die eine Gefährdung bewirken. Geht man davon aus, dass sich die Menge aller Fehl- und Betriebszustände in Zustände mit gefährlichen und mit ungefährlichen Auswirkungen einteilen lässt, so wird deutlich, dass für die Sicherheit eines Systems lediglich die Menge der gefährlichen Zustände von Bedeutung ist. In Analogie zu den zuvor genannten Zuverlässigkeitskenngrößen ergibt sich somit:

---

[44] IEC 60050-191.
[45] Rakowsky 2002.
[46] Rakowsky 2002.
[47] Rakowsky 2002.



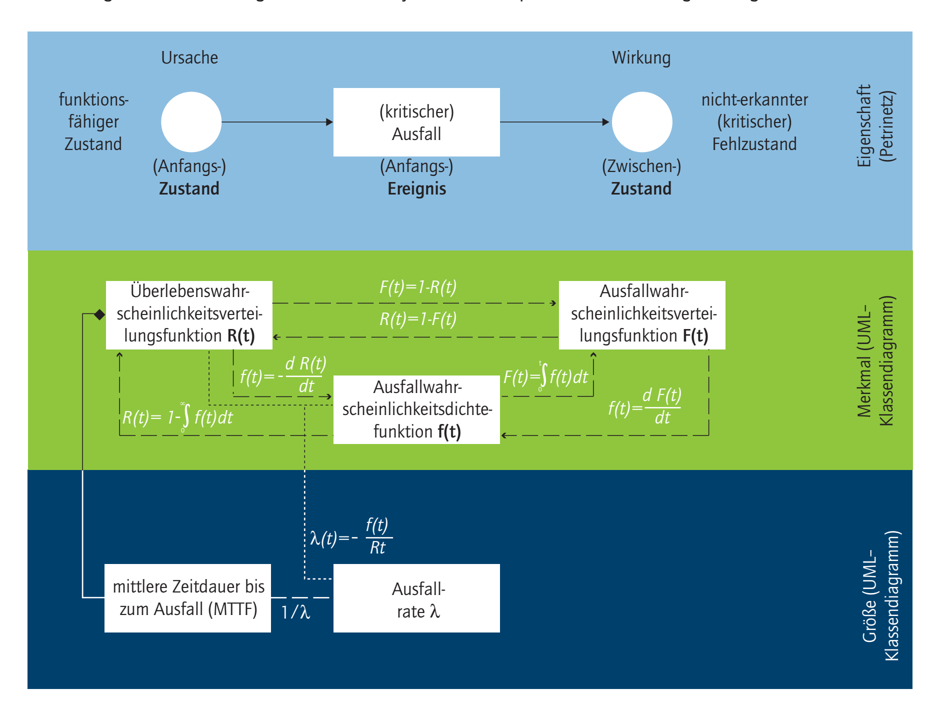



- In Bezug auf einen *kritischen Ausfall* kann die *mittlere Dauer bis zum Ausfall* in eine MTTFd (synonym hiermit MTTHE als „mean time to hazardous event") konkretisiert werden.[48]
- In Analogie zur mittleren Dauer bis zum Ausfall (MTTF) kann auch bei der Ausfallrate zwischen einer *Ausfallrate bei unkritischen Ausfällen* (λs) und einer *Ausfallrate bei kritischen Ausfällen* (λd) unterschieden werden.

Zwischen den identifizierten Größen für Zustände und Ereignisse existieren mathematische Relationen. So sind Dauern und Raten reziproke Größen. Die unterschiedlichen Raten entsprechen Komplementärwahrscheinlichkeiten; ebenso komplementär zueinander sind die identifizierten Bestandsdauern der Zustände. Abbildung 10 zeigt die formalisierte Darstellung der Merkmale und Größen des Eigenschaftsbegriffs der Zuverlässigkeit in der Kombination komplementärer Beschreibungsmittel.




Abbildung 10: Instanziierung statischer und dynamischer Aspekte des Zuverlässigkeitsbegriffs



[48] DIN EN ISO 13849-1.





3.6.1.2 INSTANZIIERUNG DES INSTANDHALTBARKEITSBEGRIFFS

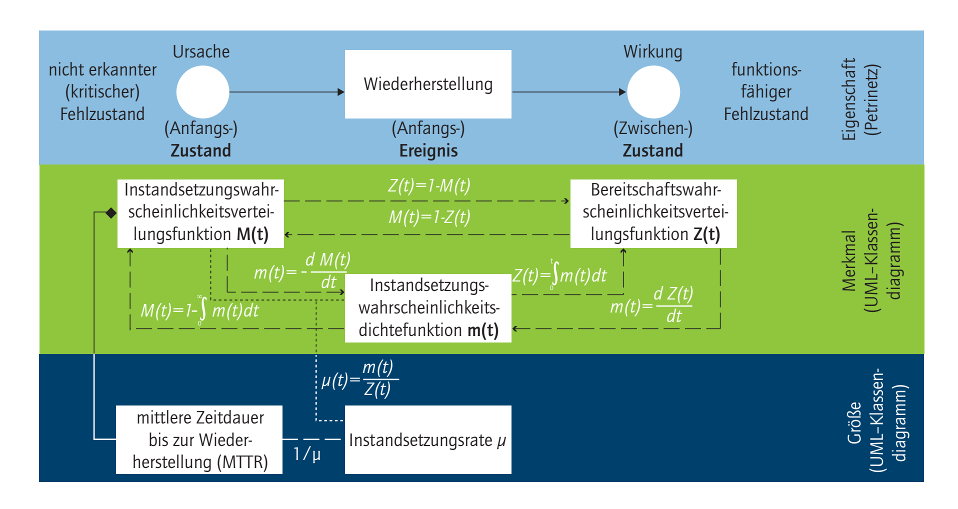
Der Begriff der Instandhaltbarkeit wird definiert als die Fähigkeit einer Einheit, unter gegebenen Anwendungsbedingungen in einem Zustand erhalten oder in ihn zurückversetzt werden zu können, in dem sie eine geforderte Funktion erfüllen kann. Hierbei wird vorausgesetzt, dass die Instandhaltung unter gegebenen Bedingungen mit den vorgegebenen Verfahren und Hilfsmitteln durchgeführt wird.[49] Für die Begriffsklärung der Instandhaltbarkeit sind ebenfalls vereinfachend die zwei komplementären Zustände der Funktionsfähigkeit und des Fehlzustands notwendig.

Der Prozess, bei dem eine Einheit vom erkannten kritischen Fehlzustand in den funktionsfähigen Zustand überführt wird, ist die Wiederherstellung oder die Instandhaltung. Der Terminus der korrektiven Instandhaltung bezeichnet „Maßnahmen nach Fehlererkennung, um eine Einheit in den funktionsfähigen Zustand zurückzuführen, so dass sie die geforderte Funktion erfüllen kann“[50] und steht in reverser Relation zum Begriff des Ausfalls.

Davon ausgehend, dass auch die Instandsetzungszeit eine Zufallsvariable ist, lässt sich in Analogie zu der zuvor behandelten Kenngröße der Ausfallwahrscheinlichkeitsverteilungsfunktion eine Instandsetzungswahrscheinlichkeitsverteilungsfunktion M(t) definieren. Die zugehörige Dichte als Instandsetzungswahrscheinlichkeitsdichtefunktion m(t) lässt sich durch die Ableitung der Verteilungsfunktion mathematisch bestimmen. Die Funktion der Instandsetzungsrate μ(t) kann in Analogie zur Ausfallrate mathematisch bestimmt werden.[51]



Abbildung 11 zeigt die formalisierte Darstellung der Merkmale und Größen des Eigenschaftsbegriffs der Instandhaltbarkeit.



49 VDI 4001.
50 IEC 60050-191.
51 Meyna/Pauli 2003.





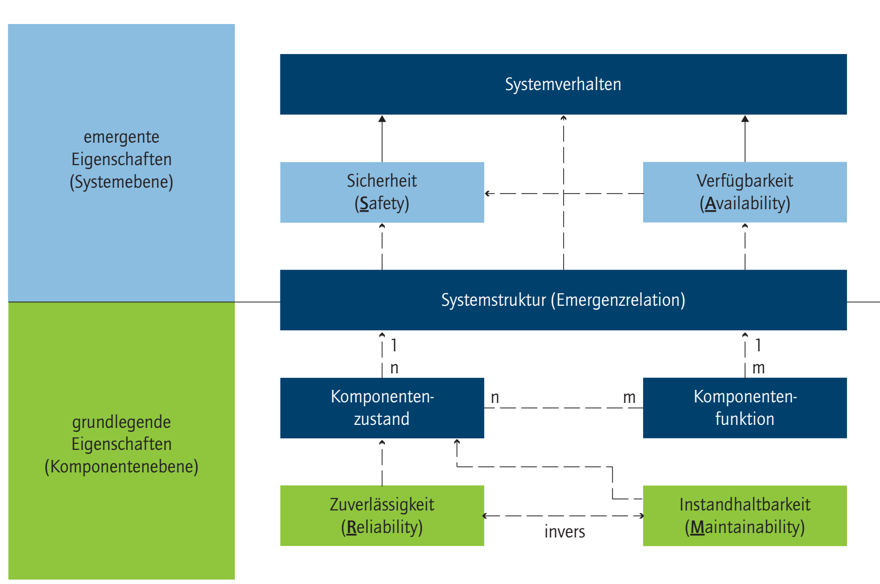
3.6.2 EMERGENTE EIGENSCHAFTEN

Sicherheit ist immer eine Eigenschaft des gesamten Systems und nicht der einzelnen Komponenten, Module, Subsysteme oder anderer nachgeordneter Betrachtungseinheiten. Beispielsweise kann ein zusätzliches Gefährdungspotenzial aus den Schnittstellen bei der Verknüpfung sicherer Einheiten zu einem Gesamtsystem (vgl. Abschnitt 3.6) entstehen. Ebenso ist es möglich, dass von einzelnen sicheren Komponenten keinerlei Gefahren ausgehen, diese jedoch bei deren Zusammenwirken entstehen.[52]

Abbildung 12 verdeutlicht, dass die Sicherheit aus dem Zusammenwirken der verschiedenen Eigenschaften (dargestellt durch die zuvor erörterten Teilbegriffssysteme) als emergente[53] Eigenschaft entsteht. Hierbei ist die Systemstruktur zu beachten, da durch die strukturelle Kopplung verschiedener Komponenten im Kontext des Gesamtsystems dieses gegebenenfalls die geforderte Funktion auch dann noch erfüllt, wenn Fehlzustände bei speziellen, bezeichneten Untereinheiten entstehen (sogenannte Fehlzustandstoleranz). Die Systemstruktur tritt somit als gleichwertige Gestaltungseigenschaft neben die grundlegenden, auf Komponentenebene wirkenden Eigenschaften der Zuverlässigkeit und Instandhaltbarkeit. Redundanz als Vorhandensein von mehr als einem Mittel in einem System zur Ausführung einer geforderten Funktion ist ein konkretes Beispiel dafür, wie die Systemstruktur zu einer Verbesserung der ermergenten Eigenschaft der Sicherheit und analog zur Verfügbarkeit beitragen kann.



Abbildung 12: Sicherheit als emergente Eigenschaft im systemischen Kontext



52 Rakowsky 2002.
53 Willke 2000.





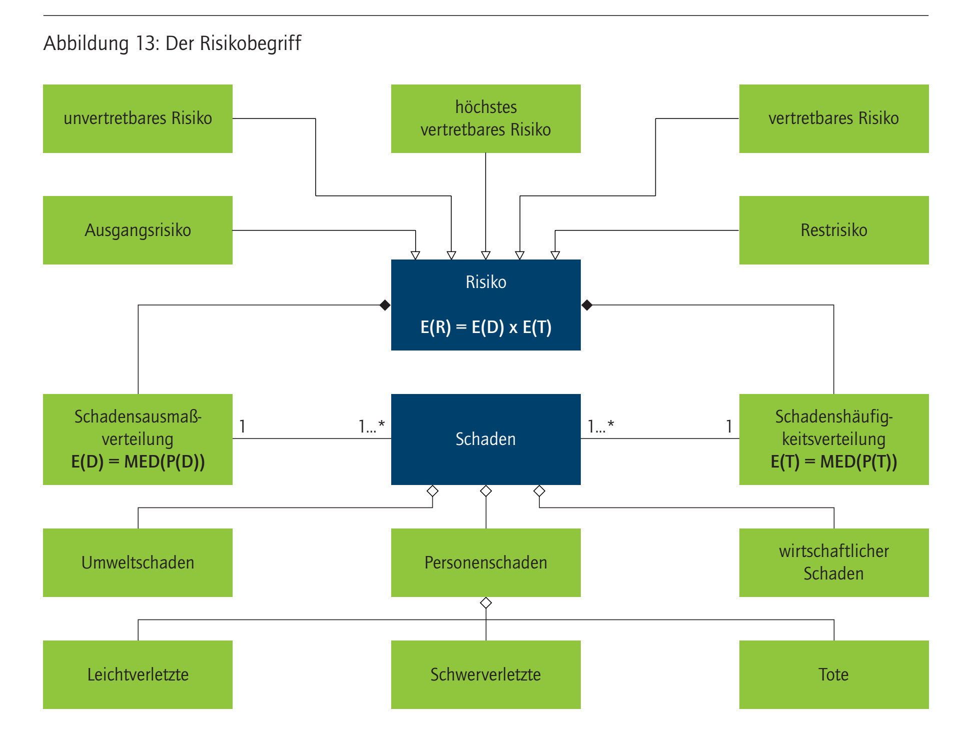
3.6.2.1 RISIKOBEGRIFF

„Sicherheit" ist kein absoluter Begriff. Sie ist in den technischen Normen zumeist als relative Sicherheit definiert, was direkt auf Akzeptanz- und Aversionsvorgaben hinweist. Sicherheit als Freisein von unvertretbarem Risiko verweist auf die Größe des Risikos. Das Risiko selbst ist eine abhängige Größe[54] und wird bezeichnet als „Kombination der Wahrscheinlichkeit, mit der ein Schaden auftritt und dem Ausmaß dieses Schadens"[55]. In dieser Definition wird der Risikobegriff als abgeleitete Größe durch die beiden Größen Schadensausmaß und Schadenshäufigkeit bestimmt. Das Risiko ist somit als mathematisches Produkt der Erwartungswerte von Schadensausmaß und -häufigkeit definiert und kann durch einen Risikowert quantitativ bestimmt werden.[56]

Die „Sicherheit" ist ein komplexer Relationsbegriff, in dem das Risiko eines Systems mit einem unvertretbaren Risiko verglichen wird, welches einen oberen Grenzwert darstellt. Der zur „Sicherheit" komplementäre Begriff ist der Begriff der Gefahr. Die „Gefahr" ist definiert als Sachlage, bei der das Risiko größer als das vertretbare Risiko ist.[57]



Abbildung 13: Der Risikobegriff



54 DIN 1313.
55 DIN IEC 61508-4.
56 Schnieder/Drewes 2008.
57 VDI 2342.





Um das „Risiko“ zu erklären, bedarf es des Begriffs des Schadens, der als Umfang oder Ausmaß der Schädigung der Gesundheit von Menschen, von Gütern oder der Umwelt definiert ist. Schäden sind stochastischer Natur und verfügen daher über eine Verteilung. In Bezug auf das beeinträchtigte Rechtsgut lassen sich die folgenden Schadenstypen identifizieren:

- *Personenschäden* sind tote, schwerverletzte oder leichtverletzte Menschen. Die Grenzen in einer solchen ordinalen Merkmalsklassifikation sind in verschiedenen Ländern unterschiedlich definiert. Als Beispiel kann die von Eurostat vorgeschlagene Einteilung gelten, wonach als Toter ein Unfallopfer gilt, dessen Tod innerhalb von 30 Tagen nach dem Unfall eintritt, wobei der Unfall Hauptgrund für das Versterben sein muss. Eine Person gilt als schwerverletzt, wenn sie mehr als 24 Stunden medizinischer Betreuung bedarf. Alle sonstigen Personenschäden sind den Leichtverletzten zuzurechnen. Hierunter fallen auch die unter Schock stehenden oder traumatisierten Personen.[58]
- *Umweltschäden* beziehen sich[59] auf die Beschädigung benachbarten Eigentums, die Freisetzung schädigender (toxischer) Substanzen oder Feuer. Für Umweltschäden existieren bislang noch keine allgemein akzeptierten Maße.
- *Wirtschaftliche Schäden* beziehen sich auf wirtschaftliche Einbußen durch Imageverluste oder stagnierendes Fahrgastaufkommen infolge des Unfalls. Da diese Effekte nur schwer zu quantifizieren sind, werden sie in der Regel nicht in Risikobetrachtungen mit einbezogen.




3.6.2.2 VORGEHENSWEISE DER RISIKOBEHERRSCHUNG

Die Sicherheitstechnik sorgt dafür, dass die Wahrscheinlichkeiten für den Eintritt und das jeweilige Ausmaß möglicher Schäden klein gehalten oder wirkungsvoll gemindert werden. Als Vergleichsmaß hat sich hierfür der zuvor diskutierte Begriff des Risikos durchgesetzt. Der zentrale Begriff für die Beherrschung von Risiken ist die „Risikobearbeitung“, welche nachfolgend dargestellt wird.

- *Risikobearbeitung:* Im Zuge eines iterativen Verfahrens von Risikobeurteilung und Risikominderung werden Schutzmaßnahmen ausgewählt und eingesetzt. Der Begriff der Risikobearbeitung wird streng gegen den Begriff des Risikomanagements[60] abgegrenzt. Letzterer schließt finanzielle, soziale, politische, kommerzielle, haftungsrechtliche und andere Wagnisse mit ein. Allerdings obliegt es einem solchen Risikomanagement, im Rahmen der Organisationspflicht die Voraussetzungen für eine ordnungsgemäße Risikobearbeitung zu schaffen.[61]

---

58 Andere Möglichkeiten der Klasseneinteilung sind in DIN05b genannt.
59 Nach CLC/TR 50126-2.
60 ISO/IEC Guide 73
61 DIN-Fachbericht 144, ISO: SMB/3971/DC.

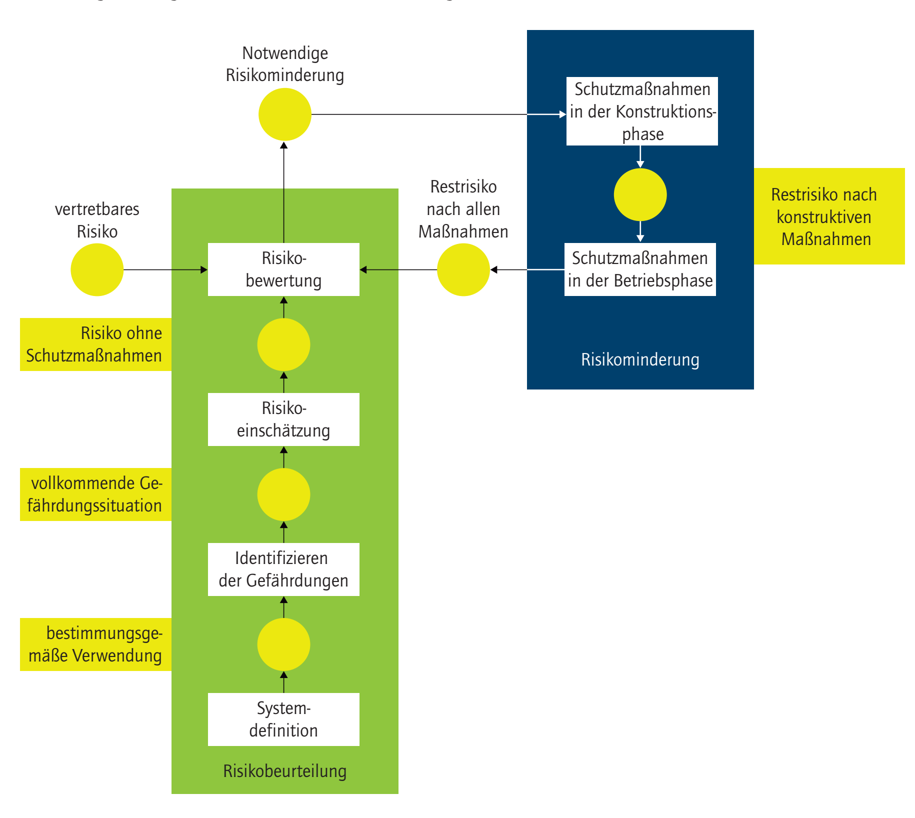




- *Risikobeurteilung:* Die Risikobeurteilung beantwortet die Frage, ob ein Produkt als sicher betrachtet werden darf. Dieses Ziel ist erreicht, wenn die Restrisiken (Risiken, die nach der Anwendung von Risikobeurteilungen und Risikominderungen verbleiben) das vertretbare Risiko (Risiko, das in einem bestimmten Zusammenhang nach den gültigen Wertvorstellungen einer Gesellschaft akzeptiert wird) unterschreiten.[62]
- *Risikominderung:* Hierunter wird das Ergreifen von Maßnahmen, die potenzielle Schadensquellen beseitigen oder das Schadensausmaß verringern, verstanden.[63] Aufgrund der unterschiedlichen Perspektiven (Sicherheit als Schutz der Umwelt vor Systemauswirkungen und Sicherheit gegen Fremdeinwirkungen) unterscheiden sich die ergriffenen Maßnahmen.

Abbildung 14: Vorgehensweise der Risikobearbeitung nach DIN-Fachbericht 144[64]



62 DIN-Fachbericht 144, ISO: SMB/3971/DC.
63 DIN-Fachbericht 144, ISO: SMB/3971/DC.
64 DIN-Fachbericht 144.





3.6.3 SAFETY AND SECURITY

In Bezug auf die Sicherheit ist zwischen zwei unterschiedlichen Sichtweisen zu unterscheiden:

- Wird die Umgebung vor den Gefahren, die vom System ausgehen, geschützt, wird dies als „Sicherheit“ (englisch: „Safety“) bezeichnet (vgl. Abschnitt 3.6.3.1). Grundlegende Dokumente hierfür sind vor allem DIN-Fachbericht 144 und ISO/IEC Guide 51.[65]
- Wird das System vor Gefahren geschützt, so wird dies als „Sicherheit gegen Fremdeinwirkungen“ (englisch: „Security“) bezeichnet (vgl. Abschnitt 3.6.3.2). Grundlegendes Dokument hierfür ist ISO: SMB/3971/DC.[66]

Das in diesem Abschnitt vorgestellte Risikokonzept sowie die Vorgehensweise der Risikobearbeitung gelten für beide Sichtweisen. Sie werden somit der Behandlung der spezifischen Terminologie der Wirkungsabläufe, die in den folgenden Abschnitten erfolgt, vorangestellt.

3.6.3.1 SCHUTZ DER UMWELT VOR SYSTEMAUSWIRKUNGEN (SAFETY)





Die Sicherheitstechnik setzt voraus, dass Risiken kausal begründet sind. Es wird hier der Versuch unternommen, ein generisches Wirkmodell für den Schadensablauf zu postulieren, auch wenn die kausalen Abhängigkeiten zwischen den einzelnen Zuständen in DIN-Fachbericht 144 und ISO/IEC Guide 51 nicht explizit enthalten sind. Abbildung 15 stellt daher den Entwurf um Inkonsistenzen bereinigten und einer formalisierten Darstellung des in DIN-Fachbericht 144 und ISO/IEC Guide 51 natürlichsprachlich (und teilweise widersprüchlich) dargestellten Wirkmodells dar.

- Eine *potenzielle Gefährdung* ist eine Situation, welche die Entwicklungsmöglichkeit zu einer Gefährdung aufweist. Diese Möglichkeit wird jedoch momentan nicht ausgeschöpft. (Dieser Terminus ist in DIN-Fachbericht 144 nicht definiert.)
- Das *Gefährdungsereignis* ist nach DIN-Fachbericht 144 ein Ereignis, das einen Schaden hervorrufen kann, es jedoch nicht muss. Aus dem Gefährdungsereignis resultiert die Gefährdung. Der Übergang in den Zustand einer Gefährdung kann mit einer Auftretensrate attributiert werden. Diese Werte können zum einen empirisch durch die Betriebserfahrung (Ermittlung aus statistischen Daten der im Bezugszeitraum erbrachten Betriebsleistung und der aufgetretenen Gefährdungen) oder auf der Basis einer theoretischen Sicherheitsanalyse[67] ermittelt werden

[65] DIN-Fachbericht 144, ISO/IEC Guide 51.
[66] ISO: SMB/3971/DC.
[67] Braband 2008.





- Die *Gefährdung* ist laut DIN-Fachbericht 144 ein Systemzustand mit Schadenspotenzial. Sie kann sich zu einem Schaden auswirken, wenn sie zeitlich und räumlich mit den unbeeinträchtigten Rechtsgütern zusammentrifft und somit eine *Gefährdungssituation* konstituiert.
- Ein weiterer für die Explikation des Sicherheitsbegriffs wesentlicher Terminus ist der Begriff der *unbeeinträchtigten Rechtsgüter*, worunter Mensch, Güter und Umwelt subsumiert werden. Dieser Begriff wird in der Normung nicht explizit genannt.
- In einer *Gefährdungssituation* sind Menschen, Güter und Umwelt einer oder mehreren Gefährdungen ausgesetzt (nach DIN-Fachbericht 144). Für den Eintritt eines Schadensereignisses ist das räumliche und zeitliche Zusammentreffen (Koinzidenz) von Gefährdung und Rechtsgütern notwendige Voraussetzung. Hierbei ist für die Quantifizierung einer Schadenseintrittswahrscheinlichkeit die Möglichkeit der Gefährdungsexposition des betreffenden Personenkreises und der anderen Rechtsgüter zu berücksichtigen.
- Der Begriff des *Schadens* umfasst ganz allgemein die Beeinträchtigung bestehender Rechtsgüter. Der Schadensbegriff ist bereits zuvor bei der Darstellung des grundlegenden Risikobegriffs in seinen verschiedenen Ausprägungen dargestellt worden.



Abbildung 15 zeigt, dass die Größe des Risikos durch multiplikative Verknüpfung der mittleren Eintrittshäufigkeit eines Schadens mit seinem mittleren Ausmaß gebildet wird. Bereits zuvor (vgl. Abschnitt 3.6.2.1) ist der Sicherheitsbegriff als komplexer Relationsbegriff erörtert worden, der sich aus dem Vergleich des tatsächlichen Risikos zum zulässigen Risiko einer technischen Einrichtung konstituiert. Der Wert des Ausgangsrisikos ist Eingangsgröße für die Risikobearbeitung (vgl. Abschnitt 3.6.2.2). Durch iterative Systementwicklung (zum Beispiel Maßnahmen der Struktur- und Parametervariation) wird das Restrisiko so lange reduziert, bis dieses den vorgegebenen Wert des vertretbaren Risikos unterschreitet. Die Schutzmaßnahmen, die bereits in der Konstruktion durchzuführen sind, werden in den anerkannten Regeln der Technik näher spezifiziert.[68]

[68] VDI Ausschuss Technische Sicherheit 2007, DIN IEC 61508.







Abbildung 15: Wirkmodell des Schadensablaufs – Sicherheit (definiert in DIN-Fachbericht 144)





3.6.3.2 SCHUTZ DES SYSTEMS VOR FREMDEINWIRKUNGEN (SECURITY)

Auch für den Bereich der Sicherheit gegen Fremdeinwirkungen setzt die Sicherheitstechnik voraus, dass die Risiken kausal begründet sind. Es wird auch hier der Versuch unternommen, ein generisches Wirkmodell für den Schadensablauf zu postulieren, auch wenn die kausalen Abhängigkeiten zwischen den einzelnen Zuständen in ISO: SMB/3971/DC nicht explizit enthalten sind. Abbildung 16 stellt daher den Entwurf einer formalisierten Darstellung des in ISO: SMB/3971/DC natürlichsprachlich (und teilweise widersprüchlich) dargestellten Wirkmodells dar. Die in Abbildung 16 verwendeten Termini werden nachfolgend erläutert:

- Eine *potenzielle Bedrohung* (englisch: Potential Threat) ist eine Situation, welche die Entwicklungsmöglichkeit zu einer Bedrohung aufweist. Diese Möglichkeit wird jedoch momentan nicht ausgeschöpft. Dieser Terminus ist in ISO: SMB/3971/DC nicht vorgesehen und definiert, wird aber für die Vollständigkeit des Terminologiegebäudes vorgeschlagen.





- Durch den *Angriff* (englisch: Attack) realisiert sich die potenzielle Bedrohung. In der Kryptografie wird unter einem „Angriff" der Versuch verstanden, ein Verschlüsselungssystem zu brechen. Dieser Terminus ist in ISO: SMB/3971/DC nicht vorgesehen oder definiert und wird ebenfalls für die Vollständigkeit des Terminologiegebäudes vorgeschlagen.
- Die *Bedrohung* (englisch: Threat) ist in Anlehnung an ISO/IEC Guide 51 als eine „potenzielle Schadensquelle" definiert.
- „Eine vom Normalzustand abweichende Situation, in der die Existenz oder das Leben und die Gesundheit von Personen gefährdet sind", wird als *„Krise"* (englisch: „Crisis") bezeichnet.[69] Die „Krise" wird hier äquivalent zum Begriff der Gefährdungssituation in DIN-Fachbericht 144 aufgefasst. Sie ist somit eine Koinzidenz der Gefährdung und der Anwesenheit der unbeeinträchtigten Rechtsgüter. Um diese Korrespondenz zum Begriff der Sicherheit (vgl. Abschnitt 3.6.3.1) stärker zum Ausdruck zu bringen, wird die Benennung *„Bedrohungssituation"* vorgeschlagen.
- Ein *Notfall* (englisch: Emergency) ist „ein Schadensereignis, bei dem Prozesse oder Ressourcen nicht wie vorgesehen funktionieren. Die Verfügbarkeit der entsprechenden Prozesse ist stark beeinträchtigt. Es entstehen hohe bis sehr hohe Schäden, die sich signifikant und in nicht akzeptablem Rahmen auf das Gesamtergebnis eines Unternehmens auswirken".[70]
- Eine *Katastrophe* (englisch: Disaster) ist „ein Schadenszustand, der zeitlich und örtlich kaum begrenzbar ist und großflächige Auswirkungen auf Menschen, Werte und Sachen haben kann. Die Existenz der Institution oder das Leben und die Gesundheit von Personen sind gefährdet. Auch das öffentliche Leben wird stark beeinträchtigt. Eine Katastrophe kann nicht ausschließlich durch die Institution selbst behoben werden".[71] Die Katastrophe ist somit eine spezielle Instanz des Schadens, welcher hinsichtlich seines Ausmaßes näher beschrieben wird.



Aufgrund der Vielfalt potenzieller Bedrohungen, die auf ein System einwirken können, wird hier exemplarisch der Schutz der Datenkommunikation vor Angriffen von außen dargestellt. Ein Beispiel für Schutzmaßnahmen, die bereits in der Konstruktion ergriffen werden können, ist der Schutz vor bösartigen Angriffen, die zum Beispiel innerhalb eines offenen Kommunikationssystems nicht ausgeschlossen werden können. Wenn nicht-authorisierte Zugriffe nicht ausgeschlossen werden, können bösartige Angriffe zwar nicht verhindert, zumindest jedoch entdeckt und in ihren Auswirkungen begrenzt werden. Es werden hierfür in DIN EN 50129 Maßnahmen, wie beispielsweise die Anwendung kryptografischer Schlüssel, gefordert.

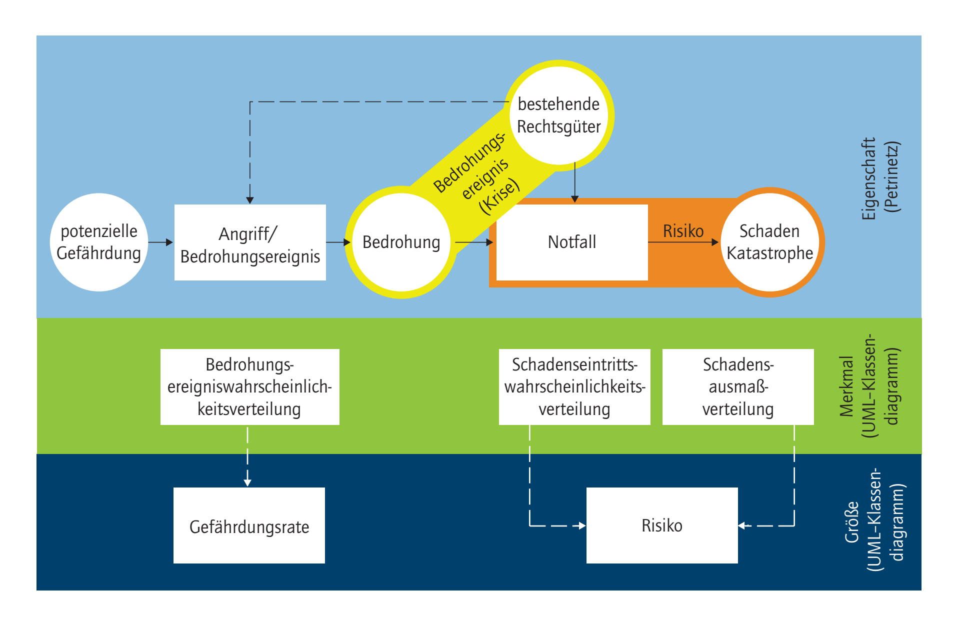
69 Vgl. BSI-Standard 100-4, ISO: SMB/3971/DC analog.
70 Vgl. BSI-Standard 100-4, ISO: SMB/3971/DC analog.
71 Vgl. BSI-Standard 100-4, ISO: SMB/3971/DC analog.







Abbildung 16: Wirkmodell des Schadensablaufs – Sicherheit gegen Fremdeinwirkungen (definiert in ISO: SMB/3971/DC)






3.7 ZUSAMMENFASSUNG

Ausgehend von der Erkenntnis, dass eine fehlerfreie Kommunikation eine zwingende Voraussetzung für die Sicherheit technischer Systeme ist, rücken zunehmend die Probleme in der allgemein- und fachsprachlichen Terminologie der Sicherheit technischer Systeme in den Mittelpunkt der Betrachtung. Zur ihrer Überwindung wurde ein neuartiger Ansatz entwickelt und thesenhaft formuliert.

- Im allgemein anerkannten Stand der Technik wurden teilweise erhebliche terminologische Defizite identifiziert und analysiert. Für den offensichtlichen Handlungsbedarf wurden Ziele definiert.
- Es wurde ein konsistenter und kohärenter methodischer Ansatz für die Zielerreichung entwickelt. Durch die aufeinander aufbauenden Schritte der Formulierung, Formalisierung, Quantifizierung, Instanziierung und Integration ermöglicht dieser Ansatz erstmals eine weiter reichende terminologische Festlegung der teilweise abstrakten Begriffe im Begriffsfeld der „Sicherheit“ als diese mit konventionellen Vorgehensweisen möglich ist.





- Das generische Modellkonzept des Begriffs und das abstrakte Modellkonzept des Systems wurden formalisiert und integriert. Das Modellkonzept des Systems liegt als Erklärungsmodell der Analyse (und Synthese) der Terminologie des Gegenstandsbereichs der Sicherheit technischer Systeme zugrunde. Es erlaubt eine Differenzierung in grundlegende und emergente Systemeigenschaften, deren Zusammenhang durch formale Beschreibungsmittel mathematisch fundiert werden kann. Oftmals lediglich umgangssprachlich verwendete Termini werden präzisiert, indem sie konsequent bis auf die Ebene empirischer oder prognostizierbarer Größen und Werte zurückgeführt werden.
- Das Resultat dieses Beitrags ist ein formalisiertes Begriffsmodell der Sicherheit. Es verbindet die oftmals isolierten Aspekte des Schutzes der Umwelt vor Systemauswirkungen (Safety) und des Schutzes des Systems vor Fremdeinwirkungen (Security). Der allgemeine Ansatz der Risikobearbeitung ist für beide Teilbegriffe im gleichen Sinne anwendbar.



Der vorliegende Beitrag soll den Blick für terminologische Unklarheiten in der Begriffswelt der „Sicherheit technischer Systeme" schärfen und zu einem problembewussten Umgang mit Sprache beitragen. Insgesamt liegt mit dem formalisierten Sicherheitsbegriffssystem sowohl eine transparente Darstellung der Begriffe als auch ein geschlossener mathematischer Zusammenhang über alle Detaillierungsebenen des Gegenstandsbereiches vor, der weitestgehend normenkonform ist. Dank der mit der Formalisierung verbundenen Zuordnung von sprachlichen Beziehungen zu Symbolen und ihrer Strukturierung ist eine wesentliche Quelle aktueller kommunikativer Missverständnisse beseitigt worden.



3.7 LITERATUR

3.7.1 NORMEN UND RICHTLINIEN

BSI-Standard 100-4
Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-4: Notfallmanagement, Bonn, 2008.

CLC/TR 50126-2
European Committee for Standardization: CLC/TR 50126-2:2007: Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 2: Guide to the application of EN 50126-1 for safety, Brüssel, 2007.





DIN 1313
DIN Deutsches Institut für Normung e. V.: DIN 1313:1998-12: Größen, Berlin, Beuth Verlag, 1998.

DIN 2330
DIN Deutsches Institut für Normung e. V.: DIN 2330:1993-12: Begriffe und Benennungen; Allgemeine Grundsätze, Berlin, Beuth Verlag, 1993.

DIN 2342:2004
DIN Deutsches Institut für Normung e. V.: DIN 2342:2004-09: Begriffe der Terminologielehre, Berlin: Beuth Verlag, 2004.

DIN EN 50129
DIN Deutsches Institut für Normung e. V.: DIN EN 50129:2003-12: Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsrelevante elektronische Systeme für Signaltechnik; Deutsche Fassung EN 50129:2003, Berlin: Beuth Verlag, 2003.

DIN EN ISO 13849-1
DIN Deutsches Institut für Normung e. V.: DIN EN ISO 13849-1:2008-12: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze (ISO 13849-1:2006); Deutsche Fassung EN ISO 13849-1:2008, Berlin, Beuth Verlag, 2008.

DIN-Fachbericht 144
DIN Deutsches Institut für Normung e. V.: DIN-Fachbericht 144: Sicherheit, Vorsorge und Meidung in der Technik, Berlin: Beuth Verlag, 2005.

DIN IEC 61508
DIN Deutsches Institut für Normung e. V.: DIN IEC 61508-4:2006-07: Funktionale Sicherheit elektrischer/elektronischer/programmierbar elektronischer sicherheitsbezogener Systeme – Teil 4: Begriffe und Abkürzungen (IEC 65A/470/CD:2005,. Berlin: Beuth Verlag, 2006.

E DIN IEC 62551
DIN Deutsches Institut für Normung e. V.: E DIN IEC 62551:2008-10: Analysemethoden für Zuverlässigkeit Petrinetz-Modellierung (Normentwurf), Berlin: Beuth Verlag, 2008.





IEC 60050-191
International Electrotechnical Commission: IEC 60050-191:1990-12: International Electrotechnical Vocabulary. Chapter 191: Dependability and quality of service, VDE Verlag, Berlin, 1990.

ISO/IEC 15909-1
International Organisation for Standardization: ISO/IEC 15909-1:2004: Software and system engineering – High-level Petri nets – Part 1: Concepts, definitions and graphical notation, Berlin: Beuth Verlag, 2004.

ISO/IEC Guide 51
International Organisation for Standardization: ISO/IEC Guide 51:1999: Safety aspects – Guidelines for their inclusion in standards, Berlin: Beuth Verlag, 1999.

ISO/IEC Guide 73
International Organisation for Standardization: ISO/IEC Guide 73:2002: Risk management – Vocabulary – Guidelines for use in standards, Berlin: Beuth Verlag, 2002.

ISO/IEC Guide 99
International Organisation for Standardization: ISO/IEC Guide 99:2007-12: International vocabulary of metrology – Basic and general concepts and associated terms (VIM), Berlin: Beuth Verlag, 2007.

ISO: SMB/3971/DC
International Organisation for Standardization: ISO: SMB/3971/DC: ISO/IEC Draft Guide: Guidelines for the inclusion of security aspects in standards, Genf, 2009.

VDI 2342
VDI Verein Deutscher Ingenieure: VDI 2342 Blatt 2:1998-07: Sicherheitstechnische Begriffe für Automatisierungssysteme – Blatt 2: Quantitative Begriffe und Definitionen, Berlin: Beuth Verlag, 1998.

VDI 4001
VDI Verein Deutscher Ingenieure: VDI 4001 Blatt 2:2006-07: Terminologie der Zuverlässigkeit, Berlin: Beuth Verlag, 2006.

VDI 4008
VDI Verein Deutscher Ingenieure: VDI 4008 Blatt 4:2008-07: Methoden der Zuverlässigkeit – Petri-Netze, Berlin: Beuth Verlag, 2008.





3.7.2 WEITERE FACHLITERATUR

Arntz/Picht/Mayer 2004
Arntz, R./Picht, H./Mayer, F.: Einführung in die Terminologiearbeit, Hildesheim: Georg Olms, 2004.

von Bertalanffy 1969
von Bertalanffy, L.: General System Theory – Foundations, Development, Application, New York: George Braziller, 1969.

Braband 2008
Braband, J. „Nachweis mindestens gleicher Sicherheit gegenüber Referenzsystemen." In: Signal + Draht 100 (2008), Nr. 12, S. 39-43.

Carnap 1959
Carnap, R.: Induktive Logik und Wahrscheinlichkeit, Wien: Springer, 1959.

Felber/Budin 1989
Felber, H./Budin, G.: Terminologie in Theorie und Praxis, Tübingen: Gunter Narr, 1989.



Hänsel 2008
Hänsel, F.: „Zur Formalisierung technischer Normen.", Fortschritt-Berichte VDI, Reihe 10, Nr. 787 (Dissertation, Institut für Verkehrssicherheit und Automatisierungstechnik), Düsseldorf: VDI Verlag, 2008.

Keller 1995
Keller, R.: Zeichentheorie: zu einer Theorie semiotischen Wissens, Tübingen: Francke, 1995.

Kortmann 1999
Kortmann, B.: Linguistik: Essentials – Anglistik, Amerikanistik, Berlin: Cornelsen, 1999.

Löbner 2002
Löbner, S.: Semantik – Eine Einführung, Berlin: de Gruyter, 2002.

Lutzeier 2007
Lutzeier, P. R.: Lexikologie, Tübingen: Stauffenberg, 2007.





Meyna/Pauli 2003
Meyna, A./P., Bernhard: Taschenbuch der Zuverlässigkeits- und Sicherheitstechnik – Quantitative Bewertungsverfahren, München: Hanser, 2003.

Ogden 1974
Ogden, C. K./Richards, I. A.: Die Bedeutung der Bedeutung, Frankfurt: Suhrkamp, 1974.

Object Management Group 2009
Object Management Group: OMG Model Driven Architecture. URL: http://www.omg.org/mda [Stand: 22.07.2009].

Rakowsky 2002
Rakowsky, U. K.: Systemzuverlässigkeit: Terminologie, Methoden, Konzepte, Hagen: LiLoLe-Verlag, 2002.

de Saussure 2001
de Saussure, F.: Grundfragen der allgemeinen Sprachwissenschaft, Berlin: de Gruyter, 2001.





van Schrick 2002
van Schrick, D.: Entepetives Management – Konstrukt, Konstruktion, Konzeption – Entwurf eines Begriffssystems zum Umgang mit Fehlern, Ausfällen und anderen nichterwünschten technischen Phänomenen, Aachen: Shaker Verlag, 2002.

Schnieder 1999
Schnieder, E.: Methoden der Automatisierungstechnik – Beschreibungsmittel, Modellkonzepte und Werkzeuge für Automatisierungssysteme, Braunschweig: Vieweg, 1999.

Schnieder 2003
Schnieder, E.: „Integration heterogener Modellwelten in der Automatisierungstechnik." In: Nagl, M./Westfechtel, B. (Hrsg.): Modelle, Werkzeuge und Infrastrukturen zur Unterstützung von Entwicklungsprozessen, Weinheim: Wiley-VCH, 2003.

Schnieder 2009
Schnieder, L.: Formalisierte Terminologien technischer Systeme und ihrer Zuverlässigkeit, (Dissertation, Fakultät für Maschinenbau der Technischen Universität Braunschweig), Braunschweig, 2009.





Schnieder/Drewes 2008
Schnieder, E./Drewes, J.: „Merkmale und Kenngrößen zur Bemessung der Verkehrssicherheit.“ In: Zeitschrift für Verkehrssicherheit 54 (2008), Nr. 3, S. 117-123.

VDI Ausschuss Technische Sicherheit 2007
VDI Ausschuss Technische Sicherheit: Qualitätsmerkmal „Technische Sicherheit“, (Denkschrift des Vereins Deutscher Ingenieure), Düsseldorf: VDI Verlag, 2007.

Vester 2002
Vester, F.: Die Kunst vernetzt zu denken – Ideen und Werkzeuge für einen neuen Umgang mit Komplexität, München: Deutscher Taschenbuch Verlag, 2002.

Willke 2000
Willke, H.: Systemtheorie I – Grundlagen, Stuttgart: Lucius & Lucius, 2000.

Wolski 1989
Wolski, W.: „Das Lemma und die verschiedenen Lemmatypen.“ In: Hausmann, F. J./ Reichmann, O./Wiegand, H. E./Zgusta, L. (Hrsg.): Handbücher zur Sprach- und Kommunikationswissenschaft, Band 5: Ein internationales Handbuch zur Lexikographie, Teilband 1, Berlin: de Gruyter, 1989, S. 360-371.





Wüster 1978
Wüster, E.: Einführung in die Allgemeine Terminologielehre und Terminologische Lexikographie, Wien: Springer, 1978.





4 THESEN ZUM PROBLEMFELD TECHNISCHE SICHERHEIT AUS JURISTISCHER SICHT

KLAUS VIEWEG

4.1 ALLGEMEINES

1. Sicherheit ist weltweit ein multidisziplinäres Thema, das es verdient, interdisziplinär behandelt zu werden.
2. Die wesentlichen (Sicherheits-) Entscheidungen werden in den Feldern Politik, Technik, Wirtschaft und Recht getroffen. Wesentliche Vorinformationen liefern die Naturwissenschaften, die Psychologie, Soziologie, Philosophie, Ethik und Geschichte. Die (Sicherheits-) Entscheidungen haben als Ausgangspunkt in der Regel unerwünschte Zustände und Ereignisse, die mit Begriffen wie „Risiko", „Gefährdung", „Gefahr" und „Schaden" beschrieben werden. Getroffen werden die (Sicherheits-) Entscheidungen nicht nach einheitlichen Methoden und Ansätzen. Diese divergieren vielmehr insbesondere nach Funktion und fachlicher Ausrichtung des Entscheidenden einerseits sowie nach Art und Ausmaß des unerwünschten Zustandes bzw. Ereignisses andererseits. Auch die Safety-Security-Diskussion ist hier zu verorten. Fokussierungen auf die eigene Fachdisziplin und vor allem die Ausblendung der in den Bereichen Politik und Recht getroffenen Entscheidungen können den Aussagewert wissenschaftlicher Ergebnisse erheblich relativieren. Hingegen dient die Schaffung von Verständigungsbrücken zwischen den verschiedenen Disziplinen der Qualität der Entscheidungsfindung und vermeidet Zeitverlust und Zusatzkosten.

4.2 VERSTÄNDIGUNG ÜBER BEGRIFFE UND SZENARIEN

1. Die verwendeten Begriffe spiegeln die unterschiedlichen Ziele und Aufgaben der verschiedenen Fachdisziplinen wider (zum Beispiel technische Maßnahmen zur Verhinderung oder Reduzierung der unerwünschten Zustände und Ereignisse oder rechtliche Vorgaben bezüglich der Beschaffenheit von Gegenständen, der Verantwortlichkeit, Zuständigkeit und Haftung von Personen und Organisationen). Die innerhalb der einzelnen Fachgebiete verwendeten Begriffe unterscheiden sich zum Teil erheblich. Selbst in den einzelnen Fachdisziplinen divergieren nicht selten die Begriffsverständnisse und Definitionen und verdecken dabei mitunter Wertungen und Abwägungen (zum Beispiel anthropozentrische Eingrenzung der Schutzgüter, Risikoakzeptanz, Ausblendung sogenannter Entwicklungsrisiken).



2. Versucht werden sollte, Arbeitsbegriffe zu finden und zu definieren, die eine interdisziplinäre – gegebenenfalls auch intradisziplinäre – und möglichst auch internationale Verständigung ermöglichen. Diese ist Voraussetzung für die Lösung der schwierigen Sachfragen. Besonderes Gewicht haben – quasi als nicht verhandelbare Vorgaben – die in der Rechtsordnung und in der technischen Normung (DIN, VDE, DKE, DVGW, CEN, CENELEC, ETSI, ISO, IEC) verwendeten Begriffe. Sie sollten aufeinander abgestimmt sein.
3. Ausgangspunkt begrifflicher Klärungen ist, dass es eine absolute, vollständige Sicherheit nicht gibt. Möglich ist nur eine relative, von den Umständen des Einzelfalls und dem Zeitablauf abhängige Sicherheit. Die Fragen sind insbesondere: „Wie sicher ist sicher genug?" und „Wer entscheidet nach welchen Prinzipien und Kriterien darüber?"
4. Die Arbeitsbegriffe müssen eine Verständigung über folgende Fragen ermöglichen:

   - Wer und/oder was ist Schutzobjekt? – Ist es der Mensch und seine (Sach-) Güter oder auch die ihm nicht zugeordnete, das heißt ungebundene Natur (Problem des sogenannten ökologischen Risikos bzw. Schadens)?
   - Wogegen soll geschützt werden? – Gegen zielgerichtete Angriffe und Eingriffe (Security) und/oder gegen sonstige negative Wirkungen durch unerwünschte Zustände und Ereignisse (Safety – technisches Versagen, menschliches und organisatorisches Versagen, Naturereignisse)? Sollen noch unbekannte, aber bei der Entwicklung neuer Technologien nicht ausschließbare unerwünschte Zustände und Ereignisse (sogenannte Entwicklungsrisiken) in den Schutz einbezogen werden?
   - Handelt es sich bei den unerwünschten Zuständen und Ereignissen um statistisch erfassbare oder zumindest schätzbare Größen oder um ein taktisch angepasstes Verhalten, einen dynamischen Prozess (zum Beispiel einen terroristischen Angriff; aber auch – als Naturereignis – die Mutationen von Viren bei Resistenzen)?
   - Soll bereits der Begriff Ausgangspunkt für die Ergreifung von Maßnahmen sein? Mit anderen Worten: Sollen bei Vorliegen von Tatsachen, die sich unter den Begriff des unerwünschten Zustandes bzw. Ereignisses subsumieren lassen, Maßnahmen ergriffen, das heißt Konsequenzen gezogen werden (zum Beispiel Realisierung technisch-organisatorischer Maßnahmen, Einschreiten einer Behörde, Verweigerung der Genehmigung des Betriebs einer Anlage, Haftung, Strafbarkeit)?






– Sollen außer dem Ausmaß des unerwünschten Zustandes bzw. Ereignisses (dem potenziellen Schadensausmaß) und der Wahrscheinlichkeit des Eintritts dieses unerwünschten Zustandes bzw. Ereignisses – diese beiden Aspekte bilden den klassischen Risikobegriff (englisch: Risk) – auch Vorteile und Chancen in die Definition einbezogen werden? Falls ja: wie? Sollen zum Beispiel Quantifizierungen ausschlaggebend sein? Soll beispielsweise bei der Abwägung zwischen dem Risiko und den Vorteilen und Chancen das Verhältnismäßigkeitsprinzip gelten?
– Sollen auch Kostenaspekte einbezogen werden? Falls ja: wie? (Quantifizierungsproblem, Abwägungsproblem).

5. Die Verständigung zwischen den verschiedenen Disziplinen und speziell das Verständnis von Gesetzgebung, Verwaltungsentscheidungen und Rechtsprechung erfordern eine Transparenz des methodischen Vorgehens.
   Deutlich werden sollten die Schritte, die in den verschiedenen Fachdisziplinen zwischen der Problemidentifikation (Risiken) und der Problemlösung (Reduzierung der Risiken) liegen. Angesichts der Vielfalt der Risiken und der Maßnahmen zu ihrer Reduzierung sind Vereinfachungen unumgänglich, um eine Verständigungsbasis zu schaffen. Vorgeschlagen wird als Orientierung die systematische Erfassung von Szenarien in einem Risiko-Raster, das gebildet wird aus den Risikoquellen – menschliches Versagen (einschließlich organisatorisches Versagen), technisches Versagen, Naturereignis, Eingriff Unbefugter – und drei idealtypischen Steuerungsmodellen der Gesetzgebung – Selbstregulierung, kooperative Steuerung und imperative Regulierung. Diese Steuerungsmodelle spiegeln die berührten (Individual- und Allgemein-) Interessen wider und entsprechen (idealiter) dem Prinzip der Verhältnismäßigkeit. Auch die exemplarisch in die Matrix aufgenommenen Maßnahmen der Risikoreduzierung sind Ausdruck von Zweckmäßigkeits- und Verhältnismäßigkeitserwägungen (siehe Abbildung 1 „Risiko-Raster“). Selbstverständlich sind Kombinationen der Risikoquellen und Abstufungen der drei Steuerungsmodelle in der Praxis verbreitet.






Abbildung 1: Risiko-Raster




STEUERUNG (BETROFFENE INTERESSEN)		RISIKOQUELLE			
		MENSCHLICHES VERSAGEN (EINSCHLIESSLICH ORGANISATORISCHES VERSAGEN)	TECHNISCHES VERSAGEN	NATUREREIGNIS	EINGRIFF UNBEFUGTER, INSBES. EXTERNER ANGRIFF
	SELBSTREGULIERUNG (EIGENINTERESSE DES GEFÄHRDETEN UND ETWAIGER VERTRAGSPARTNER)	Hausunfall, z. B. Sturz von Stuhl bei Fehlgebrauch als Leiterersatz	Kabelbrand, Verschleiß (nach Inverkehrbringen und Ablauf der Gewährleistungsfrist)	Überschwemmung des Kellers durch Starkregen; Blitzeinschlag in Eingamilienhaus (Blitzableiter nicht obligatorisch)	Einbruch in Einfamilienhaus (nur staatliche Aktion ex post)
	KOOPERATIVE STEUERUNG EU/ STAAT – UNTERNEHMEN/ PRIVATPERSONEN (ALLGEMEININTERESSE UND EIGENINTERESSE)	Bedienungsfehler, der den Verhaltensanfoderungen aufgrund des „New Approach" und des „New Legislative Framework" widerspricht	Konstruktions- oder Fabrikationsfehler, der den Beschaffenheitsanforderungen aufgrund des „New Approach" und des „New Legislative Framework" widerspricht	Blitzschlag/ Hochwasser in genehmigungsbedürftiger Anlage § 3 Abs. 2 Nr. 2 i.V.m. § 9 Abs. 1 Nr. 2 Störfall-VO (Bezugnahme in Vollzugshilfe [9.2.6.1.2 i.V.m. Anhang 1 1.2.1.1 und 1.2.2])	Zielgerichtete Verursachung eines Störfalls in einer genehmigungsbedürftigen Anlage § 3 Abs. 2 Nr. 3 i.V.m. § 9 Abs. 1 Nr. 2 Störfall-VO Leitfaden SFK-GS-38 (Bezugnahme in Vollzugshilfe [9.2.6.1.3 i.V.m. Anhang 1 1.5])
	EUROPÄISCHE/ STAATLICHE IMPERATIVE REGELUNG (ERHEBLICHES ALLGEMEININTERESSE)	Verstoß z. B. gegen: – Alkoholverbot für Fahranfänger (§ 24c StVG) – 0,5 Promille-Grenze Kfz-Führer (§ 24a StVG) – Fachkundenachweise – Pflicht, Schutzausrüstung zu tragen (§ 21a StVO: Sicherheitsgurte, Schutzhelme)	Risikoquellen werden erfasst vom (anlagenbezogenen) Sicherheitsbericht gemäß § 9 Störfall-VO; betroffen sind ca. 7.800 Anlagen i.S.v. § 3 Abs. 5 BImSchG in Deutschland	- Erdbeben: Auslegung genehmigungsbedürftiger Anlagen (§ 5 Abs. 1 Nr. 1 Störfall-VO) Blitzschlag: Blitzableiter für Versammlungsstätten (Art. 38 Abs. 3 Nr. 4 LStVG; Art. 44 BayBO) – Brandschutz für alle Gebäude – Hochwasserschutz (Bauverbot; Dammhöhe)	Zielgerichtete Verursachung eines Störfalls in einer genehmigungsbedürftigen Anlage § 3 Abs. 2 Nr. 3 i.V.m. § 9 Abs. 1 Nr. 2 Störfall-VO (Bezugnahme in Vollzugshilfe [13.3])





Weitere Differenzierungen und Varianten des – recht groben – Risiko-Rasters sind möglich. Im Einzelfall ist zu prüfen, ob die Berücksichtigung zusätzlicher Aspekte hilfreich ist. So kann die Differenzierung nach den Steuerungsinstrumenten zwischen strafrechtlicher Verantwortlichkeit, zivilrechtlicher Haftung und öffentlich-rechtlichen Pflichten zweckmäßig im Hinblick auf die Verhaltenssteuerung sein. Sie geht ins Leere bei gezielten Eingriffen Unbefugter (insbesondere bei terroristischen Angriffen). Die Differenzierung nach dem Willen des Schädigers – gewollt oder ungewollt – führt hingegen wenig weiter, da die wichtigsten Fälle gewollter Schadenszufügung sich bereits als Eingriff Unbefugter im Risiko-Raster wiederfinden.

Das Risiko-Raster kann sowohl als Informationsbasis als auch als Prüfstein für die Vollständigkeit einer querschnittlichen Systemtheorie dienen. Das Risiko-Raster macht mit der Erwähnung des New Approach und des New Legislative Framework auch die Funktion der technischen Normung deutlich, die in der Praxis in weiten Bereichen eine nicht zu unterschätzende Bedeutung dadurch erlangt hat, dass der europäische Gesetzgeber die Konkretisierung seiner allgemein gehaltenen Sicherheitsanforderungen den Normungsorganisationen CEN, CENELEC und ETSI übertragen hat.

4.3 AUFGABEN UND VERANTWORTLICHKEITEN




1. Das gemeinsame Ziel Sicherheit wird zweckmäßigerweise durch eine Verteilung der Aufgaben und Verantwortlichkeiten nach Fachqualifikation und Interesse verfolgt. Diese Verteilung erfolgt auf unterschiedliche Weise. Wesentlich ist insofern, ob die gesetzlichen Regelungen eine Selbstregulierung erlauben oder konkrete Vorgaben enthalten. Zu beachten ist die Einflussnahme von Lobbygruppen.

   – Die Fälle der Selbstregulierung sind dadurch gekennzeichnet, dass das Eigeninteresse des Gefährdeten im Vergleich zum Allgemeininteresse derart im Vordergrund steht, dass der Gesetzgeber nicht aktiv wird, sondern den allgemeinen rechtlichen Rahmen (Vertragsrecht, deliktische Haftung, strafrechtliche Verantwortlichkeit) für ausreichend erachtet. Die Verteilung der Aufgaben und Verantwortlichkeiten erfolgt bilateral auf vertraglicher Grundlage zwischen demjenigen, der sich einem von ihm nicht gewünschten Risiko ausgesetzt sieht, und demjenigen, von dem er annimmt, dass er in der Lage ist, dieses Risiko auszuschließen oder zumindest auf ein für ihn akzeptables Maß zu senken (zum Beispiel Überprüfung elektrischer Endgeräte durch einen Fachmann, Installation eines Blitzableiters gegen Blitzschlag oder einer Alarmanlage als Einbruchsicherung für ein Einfamilienhaus). Beruht das Risiko allein auf einem menschlichen Versagen des Gefährdeten selbst, so kommt als wirtschaftliche Absicherung des Risikos auch eine Versicherungslösung in Betracht.



- Die Verteilung der Aufgaben und Verantwortlichkeiten erfolgt tri- oder multilateral, wenn das Risiko über den individuellen Bereich hinausgeht und insbesondere (schutzbedürftige) Dritte und deren (Sach-) Güter sowie Allgemeingüter und -interessen betroffen sein können (zum Beispiel beim Brandschutz). In aller Regel gibt es in diesen Fällen gesetzliche Regelungen, die das konkrete Risiko betreffen. Insbesondere sind Vorgaben hinsichtlich der Zuständigkeit von Behörden und Gerichten, der strafrechtlichen Verantwortlichkeit und der zivilrechtlichen Haftung zu berücksichtigen.

2. Soweit die Verteilung der Aufgaben und Verantwortlichkeiten durch gesetzliche Vorgaben (tri- oder multilateral) erfolgt, sind idealiter zwei legislatorische Steuerungsansätze voneinander zu unterscheiden. Zum einen spielt die „klassische“ imperative Regelung durch konkrete Gebote und Verbote nach wie vor sowohl auf nationaler als auch auf europäischer Ebene eine wichtige Rolle. Sie kommt insbesondere dann zum Tragen, wenn erhebliche Allgemeininteressen (oder individuelle Rechtsgüter von besonderem Gewicht) berührt sind. Zum anderen nimmt die Bedeutung der kooperativen Steuerung zwischen EU bzw. Staat einerseits und den betroffenen Unternehmen und Privatpersonen andererseits zu. Besonders praxisrelevant sind der „New Approach“ (1985) und das „New Legislative Framework“ (2008). Typischerweise liegen der kooperativen Steuerung sowohl Allgemein- als auch Eigeninteressen der Regelungsadressaten zugrunde. Die in Teilen der Wissenschaft und Praxis vorgenommene Differenzierung zwischen sogenannten Safety- und Security-Problemen hat in den gesetzlichen Regelungen bisher keinen vollen Niederschlag gefunden (zum Beispiel fehlt noch eine Spezialregelung im Hinblick auf terroristische Angriffe auf Kernkraftwerke). Hierfür dürften zwei Gründe maßgeblich sein: zum einen ein Nachhinken der Rechtsordnung, das man als „legal lag“ bezeichnen kann (spätestens seit dem 11. September 2001 steht fest, dass durch Strafandrohung terroristische Angriffe nicht verhindert werden können), und zum anderen ein übergreifendes legislatorisches Schutzkonzept, das nicht – nach der Risikoquelle – zwischen „Safety“ und „Security“ unterscheidet, sondern den Rechtsgüterschutz als Ganzes im Blick hat.



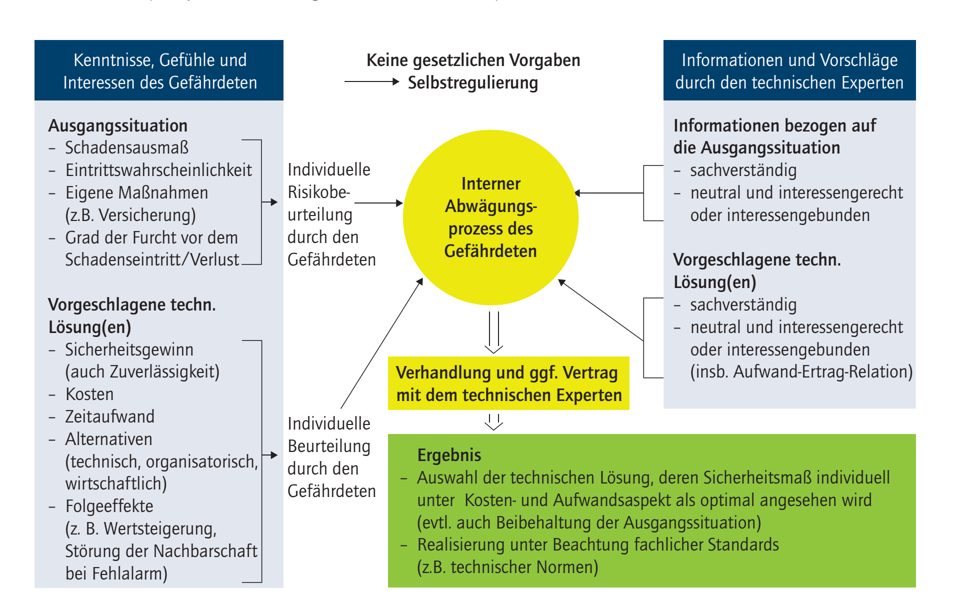




4.4 ENTSCHEIDUNGSPROZESSE

1. Im Rasterfeld, das durch das Steuerungsmodell der Selbstregulierung (betroffen sind vor allem Eigeninteressen) und die Risikoquelle des Eingriffs Unbefugter gebildet wird, lässt sich der Entscheidungsprozess (Eigenentscheidung des Gefährdeten) wie folgt kennzeichnen (siehe auch Abbildung 2 „Bilaterale Sicherheitslösung bei individueller Gefährdung"):

Abbildung 2: Bilaterale Sicherheitslösung bei individueller Gefährdung
(Beispiel: Alarmanlage für Einfamilienhaus)



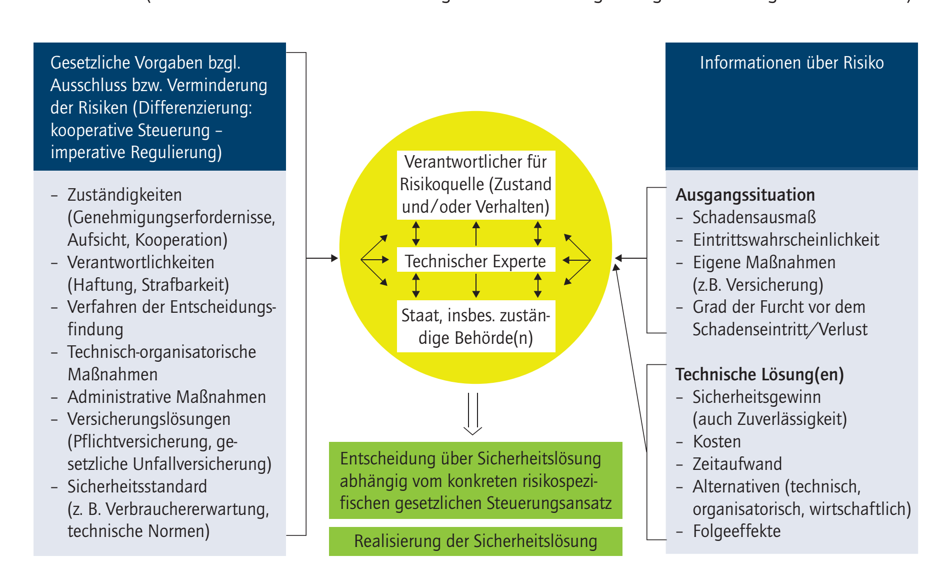



Kenntnisse, Erfahrungen, Gefühle und Interessen des Gefährdeten prägen dessen individuelle Risikobeurteilung, für die Schadensausmaß, Eintrittswahrscheinlichkeit, eigene Maßnahmen (wie Versicherung) und der Grad der Furcht vor dem Schadenseintritt maßgeblich sind. Hinzu kommen die diesbezüglichen Informationen durch den zur Beratung herangezogenen technischen Experten. Die vom technischen Experten unterbreiteten technischen Lösungsvorschläge werden durch den Gefährdeten ebenfalls individuell unter den Aspekten Sicherheitsgewinn, Kosten, Zeitaufwand, Alternativen und Folgeeffekte beurteilt. Zentral ist ein interner Abwägungsprozess des Gefährdeten. Seine Verhandlungen mit dem technischen Sachverständigen können als Ergebnis – in Vertragsform – die Auswahl der technischen Lösung beinhalten, deren Sicherheitsmaß er individuell unter dem Kosten- und Aufwandsaspekt als optimal ansieht. Bei negativer Entscheidung bleibt es bei der risikoreicheren Ausgangssituation.



2. In den Rasterfeldern, die gebildet werden durch die Steuerungsmodelle der kooperativen Steuerung und der europäischen bzw. nationalen imperativen Regulierung einerseits und den Risikoquellen des technischen Versagens, des Naturereignisses und des Eingriffs Unbefugter andererseits, lässt sich der Entscheidungsprozess hinsichtlich der Sicherheitslösung (vereinfacht) wie folgt kennzeichnen (siehe Abbildung 3 „Tri-/multilaterale Sicherheitslösung bei überindividueller Gefährdung"):

Abbildung 3: Tri-/multilaterale Sicherheitslösung bei überindividueller Gefährdung
(insbesondere Dritter und deren Sachgüter sowie von Allgemeingütern und Allgemeininteressen)






Der Entscheidungsprozess wird zum einen wesentlich beeinflusst durch die gesetzlichen Vorgaben, die bezüglich des Ausschlusses bzw. der Verminderung der Risiken bestehen. Hierzu gehören die Vorgaben hinsichtlich der Zuständigkeiten, der Verantwortlichkeiten, des Verfahrens der Entscheidungsfindung, der in Betracht kommenden technisch-organisatorischen sowie administrativen Maßnahmen, der Versicherungslösungen sowie – vor allem – des Sicherheitsstandards. Zum anderen spielen auch bei dieser Entscheidung die Informationen über das Risiko – konkret: über die Ausgangssituation sowie die technischen Lösungsmöglichkeiten – eine wesentliche Rolle. Sowohl die gesetzlichen



Vorgaben als auch die Informationen über das Risiko beeinflussen die Kommunikation und Kooperation zwischen dem Verantwortlichen für die Risikoquelle, dem technischen Experten und dem Staat, insbesondere dessen zuständigen Behörden. Die Entscheidung über die Sicherheitslösung ist dabei abhängig vom konkreten risikospezifischen gesetzlichen Steuerungsansatz.

3. Aus der Warte eines – insbesondere europäischen oder nationalen – Regelungsgebers stellt sich ein systematisches Vorgehen hinsichtlich eines konkreten Risikos (zum Beispiel eines terroristischen Angriffs auf ein Kernkraftwerk oder eine genehmigungsbedürftige Anlage) wie folgt dar:

   - Identifizierung des Risikos bzw. der Risiken und Entscheidung über den Regelungsbedarf;
   - Formulierung des Sicherheitsziels für das konkrete Szenario im Rahmen des Gesetzeszwecks;
   - Festlegung des Steuerungsansatzes anhand der berührten Interessen und des Grundsatzes der Verhältnismäßigkeit;
   - Ermittlung der in Betracht kommenden präventiven, kompensatorischen und repressiven Maßnahmen zur Beseitigung bzw. Reduzierung der Risiken (zum Beispiel technische oder administrative Maßnahmen, Benutzerinformation);
   - Festlegung der Aufgaben und Verantwortlichkeiten der Entscheidungsträger (Behörden, Industrie allgemein, konkrete Hersteller und Zulieferer, Normungsorganisationen, technische Sachverständige, Betreiber/Nutzer/Verbraucher);
   - Steuerung des Verhaltens der Entscheidungsträger (zivilrechtliche Haftung, Kosten aufgrund administrativer Maßnahmen wie zum Beispiel Rückruf, Strafbarkeit, Ansehensverlust);
   - Festlegung der Maßnahmen zur Beseitigung bzw. Reduzierung der Risiken (zum Beispiel technischer oder administrativer Maßnahmen, Benutzerinformation) aufgrund der Risikobewertung.

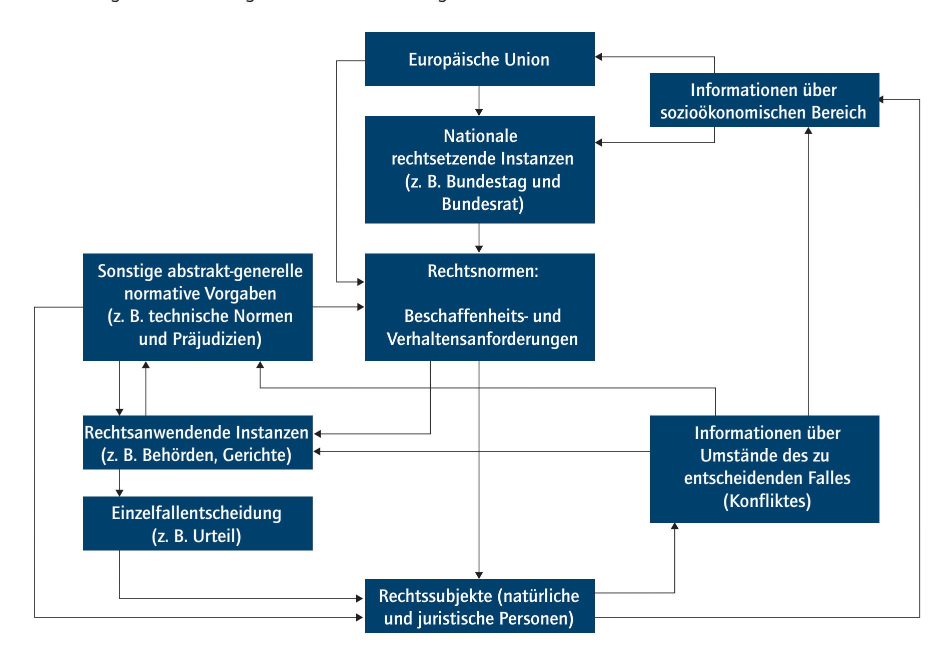



Klärungsbedarf besteht hinsichtlich der Frage, ob den bisherigen Regelungen ein solches systematisches Vorgehen zugrunde liegt und ob insbesondere dem verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit Rechnung getragen wird. Unabhängig davon trägt die Transparenz des Vorgehens zum wechselseitigen Verständnis aller Beteiligten bei. Die Schwierigkeiten des Regelungsgebers werden deutlich, wenn man die Zusammenhänge in einem Regelkreis-Modell (siehe Abbildung 4 „Rechtsetzung und Rechtsanwendung) betrachtet.





Abbildung 4: Rechtsetzung und Rechtsanwendung






4.5 ZUSAMMENFASSUNG UND EMPFEHLUNGEN

1. Als interdisziplinäre und internationale Thematik ist die Sicherheit auf Verständigung über Begriffe und methodisches Vorgehen angewiesen. Verständigungsprobleme führen zu Zeitverlust, verursachen Zusatzkosten und mindern häufig die Qualität der Entscheidungsfindung.
2. Vorgeschlagen wird, vom Arbeitsbegriff „Risiko" auszugehen, der durch die Merkmale „(potenzielles) Schadensausmaß" und „Eintrittswahrscheinlichkeit" definiert wird. Hiervon ausgehend, können begriffliche Differenzierungen und eine Strukturierung der Begriffsbeziehungen vorgenommen werden, die die Verständigung in zweckmäßiger Weise erlauben. Die Begriffsdifferenzierungen betreffen insbesondere die Pflicht, Maßnahmen zu ergreifen, und die Aussage, dass keine Maßnahmen ergriffen werden müssen, weil das Risiko akzeptabel ist. Begrifflich klargestellt werden kann weiterhin, ob Vorteile und Chancen auf dem Wege der Abwägung bei der Entscheidungsfindung berücksichtigt werden dürfen.





Wünschenswert wäre eine Zusammenstellung der im Zusammenhang mit der Sicherheitsproblematik verwendeten Begriffe und deren Zuordnung zueinander. Diese Zusammenstellungen sollten – mit Blick auf die Praxis der Entscheidungsfindung – in den drei Schlüsselbereichen Technik, Recht und Wirtschaft erfolgen, und zwar sowohl auf nationaler als auch auf internationaler Ebene. Hierbei könnte der Bereich Technik durch die technische Normung, der Bereich Recht durch Gesetzgebung, Verwaltung und Rechtsprechung und der Bereich Wirtschaft durch die Versicherungswirtschaft und Unternehmensverbände repräsentiert werden. Mit dem DIN-Fachbericht 144 und den Arbeitsergebnissen der Arbeitsgruppe „Taxonomie" sind insofern bereits wertvolle Vorarbeiten geleistet worden. Weitere Informationen zu diesem Thema enthält der Beitrag *Sicherheits- und Risikoterminologie im Spannungsfeld zwischen Recht und Technik* von Thomas Regenfus und Klaus Vieweg in diesem Band.
Auf Grundlage dieser Zusammenstellungen wäre in einem zweiten Schritt zu klären, ob die Begriffe innerhalb der Bereiche und auch interdisziplinär sowie international konsistent verwendet und verstanden werden oder ob Harmonisierungsbedarf besteht.




3. Hinsichtlich des methodischen Vorgehens, das die (Sicherheits-) Entscheidungen kennzeichnet, wird – als Verständigungshilfe – vorgeschlagen, von einem Risiko-Raster auszugehen, das durch die vier Risikoquellen – menschliches Versagen (einschließlich organisatorisches Versagen), technisches Versagen, Naturereignis, Eingriff Unbefugter – sowie durch die drei idealtypischen rechtlichen Steuerungsmodelle – Selbstregulierung, kooperative Steuerung und imperative Regelung – gebildet wird. Wünschenswert wären insofern Zusammenstellungen des methodischen Vorgehens in den auf diese Weise gebildeten zwölf Rasterfeldern. Auch hier kommt für den Bereich der Technik, der technischen Normung und in den noch nicht von der technischen Normung erfassten Risikobereichen den führenden Sicherheitsexperten eine wesentliche Bedeutung zu. Eine wichtige Vorarbeit ist zum einen in den Normungsorganisationen und zum anderen in der acatech-Arbeitsgruppe „Herstellung von Systemfähigkeit" geleistet worden. Weiterhin sind Gesetzgebung, Verwaltung und Rechtsprechung sowie die Versicherungswirtschaft und die Unternehmensverbände wesentlich. Auf Grundlage dieser Zusammenstellungen wäre zu klären, ob und inwieweit die methodischen Vorgehensweisen einander entsprechen oder ob hier Harmonisierungs- oder zumindest Klärungsbedarf besteht. Dabei sind auch branchen- und produktspezifische Lösungsansätze in den Blick zu nehmen.





4.6 LITERATUR

BMBU 2004
Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit: Vollzugshilfe zur Störfall-Verordnung vom März 2004. URL: http://www.bmu.de/files/broschueren/faltblaetter/application/pdf/vollzugshilfe_stoerfall_vo.pdf.

DIN 2005
Deutsches Institut für Normung e.V. (Hrsg.): Sicherheit, Vorsorge und Meidung in der Technik, DIN-Fachbericht 144, Berlin: Beuth Verlag, 2005.

DIN 2008
Deutsches Institut für Normung e.V. (Hrsg.): Sicherheitsgerechtes Gestalten technischer Erzeugnisse, DIN 31000 (VDE 1000), Berlin: Beuth Verlag, 2008.

DKE 2008
Deutsche Kommission Elektrotechnik Elektronik Informationstechnik (DKE) im DIN und VDE (Hrsg.): Sicherheitsgerechtes Gestalten technischer Erzeugnisse, Sonderdruck (Auszüge aus DIN 31000 (VDE 1000) und andere), Berlin: VDE Verlag/Beuth Verlag, 2008.




Dietz/Regenfus 2006
Dietz, F./Regenfus, T.: „Risiko und technische Normung im Spannungsfeld von Recht und Technik. In: Vieweg, K. (Hrsg.): Risiko – Recht – Verantwortung, Köln, Berlin, Bonn, München: Carl Heymanns Verlag, 2006, S. 403-429.

Di Fabio 1996
Di Fabio, U.: „Produktharmonisierung durch Normung und Selbstüberwachung“, Köln, Berlin, Bonn, München: Carl Heymanns Verlag, 1996.

Hosemann 2007
Hosemann, G.: „Risikobeurteilung zur Konkretisierung staatlicher Vorschriften“. In: etz (2007), Nr. 12, S. 76-81.

Intertek Research and Testing Centre et al. 2005
Intertek Research and Testing Centre et al.: „Produktsicherheit in Europa – Ein Leitfaden für Korrekturmaßnahmen einschließlich Rückrufe“. In: Geiß, J./Doll, W. (Hrsg.): Geräte- und Produktsicherheitsgesetz (GPSG) – Kommentar und Vorschriftensammlung, Stuttgart: Kohlhammer, 2005, S. 366 ff.

Marburger 1976
Marburger, P.: Regeln der Technik im Recht, Köln, Berlin, Bonn, München: Carl Heymanns Verlag, 1976.



Vieweg 1980
Vieweg, K.: „Gesamtdiskussion“. In: Lukes, R. (Hrsg.): Gefahren und Gefahrenbeurteilungen im Recht, Teil I, Köln, Berlin, Bonn, München: Carl Heymanns Verlag, 1980, S. 177-201.

Vieweg 1993
Vieweg, K.: „Recht und Risiko“. In: GSF-Forschungszentrum für Umwelt und Gesundheit (Hrsg.): mensch + umwelt, 8. Aufl. Neuherberg, 1993, S. 47-52.

Vieweg 1997
Vieweg, K.: „Reaktionen des Rechts auf Entwicklungen in der Technik“. In: Schulte, M. (Hrsg.): Technische Innovation und Recht – Antrieb oder Hemmnis? Heidelberg: C.F. Müller, 1997, S. 35-54.

Vieweg 1999
Vieweg, K.: „Technik und Recht“. In: Berlin-Brandenburgische Akademie der Wissenschaften/Nordrhein-Westfälische Akademie der Wissenschaft (Hrsg.): Technik und Technikwissenschaften – Selbstverständnis, Gesellschaft, Arbeit, Beiträge zum Arbeitssymposium des Konvents für Technikwissenschaften (KTW), Berlin, Düsseldorf, 1999 – Tagungsband. Auch abgedruckt in Vieweg, K./Haarmann, W. (Hrsg.): Beiträge zum Wirtschafts-, Europa- und Technikrecht – Festgabe für Rudolf Lukes zum 75. Geburtstag, Köln/Berlin/Bonn/München, Carl Heymanns Verlag, 2000, S. 199-213.



Vieweg 2000
Vieweg, K. (Hrsg.): Techniksteuerung und Recht – Referate und Diskussionen eines Symposiums an der Universität Erlangen-Nürnberg, Köln, Berlin, Bonn, München: Carl Heymanns Verlag, 2000.

Vieweg 2001
Vieweg, K.: „Sicherheitsgesetzbuch als Instrument zur Straffung des Technikrechts?“ In: TÜV Saarland-Stiftung (Hrsg.): Congress Documentation of the World Congress Safety of Modern Technical Systems, Köln: TÜV-Verlag, 2001, S. 473-478.

Vieweg 2006
Vieweg, K. (Hrsg.): Risiko – Recht – Verantwortung, Köln, Berlin, Bonn, München: Carl Heymanns Verlag, 2006.







5 SICHERHEITS- UND RISIKOTERMINOLOGIE IM SPANNUNGSFELD VON TECHNIK UND RECHT

THOMAS REGENFUS/KLAUS VIEWEG

5.1 EINLEITUNG

Sicherheit und Risiko sind nicht nur Begriffe der Alltagssprache. Sie finden sich auch in den Fachsprachen der Technik und des Rechts und sind dort jeweils in einen Kranz weiterer Begriffe wie Gefahr, Gefährdung, Safety, Security, Restrisiko, Risikomanagement und Schaden eingebettet.

Geht man davon aus, dass die Entwicklung und Anwendung von Technik zwangsläufig mit Risiken verbunden ist – eine absolute Sicherheit gibt es nicht – und dass wesentliche Entscheidungen auf rechtlichen Vorgaben beruhen, so folgt daraus, dass den Verständigungsbrücken zwischen den Disziplinen „Technik" und „Recht" eine ganz besondere Bedeutung zukommt. Mit anderen Worten: Sollen Fehlinvestitionen aufgrund negativer Zulassungsentscheidungen und/oder fehlender Marktfähigkeit sowie Schadensersatzpflichten bei fehlerhaften Produkten und im äußersten Fall strafrechtliche Verurteilungen vermieden werden, so müssen Entwicklung und Anwendung von Technik die rechtlichen Vorgaben im Blick haben.

Im Bereich der Technik, insbesondere in dem der technischen Sicherheit, hat die technische Normung eine Bedeutung erreicht, die kaum zu überschätzen ist. Sie bildet quasi synaptische Verbindungen an den Nahtstellen von Technik und Recht. Ihre praktische Relevanz zeigt sich am Umfang der Normenwerke, an der Anerkennung im Rahmen des Normenvertrages der Bundesregierung mit dem DIN und seit nunmehr über zwei Jahrzehnten auf europäischer Ebene zunächst am „New Approach" und seit 2008 am „New Legislative Framework".

Angesichts dieser praktischen Relevanz ist der im Jahre 2005 vom DIN mit Blick auf europäische Rechtsakte herausgegebene Fachbericht 144 „Sicherheit, Vorsorge und Meidung in der Technik", ein exzellenter Prüfstein, um herauszufinden, ob und inwieweit die Sicherheits- und Risikoterminologie in einem ganz wesentlichen Bereich der Technik mit der des Rechts in Einklang zu bringen ist und welche Bedeutung wirtschaftliche Überlegungen dabei haben können.

Im Folgenden werden – basierend auf einer umfangreicheren und mit einem wissenschaftlichen Apparat versehenen Untersuchung von *Dietz* und *Regenfus* – die Ziele und der Inhalt des DIN-Fachberichts 144 (dazu 5.2) sowie die zu bewältigenden Zielkonflikte (dazu 5.3) dargestellt, bevor aus rechtlicher Sicht die Terminologie auf Übereinstimmun-



gen und Divergenzen untersucht wird (dazu 5.4). Hierbei kann es sich aus Raumgründen nur um eine Skizzierung der Problematik handeln, die sich zudem auf die nationale Ebene beschränken muss, dabei aber bereits den weiter gehenden Forschungsbedarf erkennen lässt.

5.2 ZIELE UND INHALT DES DIN-FACHBERICHTS 144 „SICHERHEIT, VORSORGE UND MEIDUNG IN DER TECHNIK"

5.2.1 AUFGABENBESCHREIBUNG, SYSTEMATIK UND BEGRIFFSDEFINITIONEN

Der DIN-Fachbericht 144 „Sicherheit, Vorsorge und Meidung in der Technik" soll einen Beitrag zu der von der Europäischen Kommission angeregten Diskussion über die Anwendung des Vorsorgeprinzips aus Sicht der Normenersteller und -anwender leisten. Da Risikobeurteilungen in zahlreichen Zweigen der Technik erforderlich sind, soll der Fachbericht 144 eine möglichst allgemeingültige methodische Grundlage zur Durchführung von Risikobeurteilungen und -minderungen zur Verfügung stellen. Er strebt daher eine „verständliche logische Systematik" sowie eine „allgemein anwendbare anerkannte Terminologie" an. In terminologischer Hinsicht greift er auf die bereits vorhandenen Begriffsdefinitionen der DIN 820-120 und der deutschen Umsetzung des ISO/IEC-Guide 51 zurück.




Der Fachbericht 144 unterscheidet drei Bereiche des Umgangs mit Risiken, nämlich *Sicherheit, Vorsorge* und *Meidung*. Wichtig ist ferner die Gegenüberstellung von *Risikobearbeitung* und *Risikomanagement*.

Unter *Sicherheit* eines Produkts versteht der Fachbericht 144 – entsprechend einem verbreiteten Begriffsverständnis – die „Freiheit von unvertretbaren Risiken". Da nur sichere Produkte auf den Markt gebracht werden dürfen, muss das naturwissenschaftlich nachweisbare Risiko – ohne Rücksicht auf mit dem Einsatz verbundene Chancen (verstanden als Oberbegriff für Vorteile, Nutzen und andere positive Effekte sowie Erwartungen) – so lange gemindert werden, bis es vertretbar ist.

Risiko ist nach den Definitionen der DIN 820-120 und des ISO/IEC-Guide 51 die Kombination aus Wahrscheinlichkeit des Schadenseintritts und Schadensausmaß. Die Berücksichtigung von Chancen sowie deren Verrechnung mit den Nachteilserwartungen finden nicht statt.

Die Begriffe *Gefahr* und *Sicherheit* korrespondieren insofern, als sie einmal die Anwesenheit, das andere Mal die Abwesenheit eines unvertretbaren Risikos bezeichnen. Für die Vertretbarkeit des Risikos ist entscheidend, ob es „in einem bestimmten Zusammenhang nach den gültigen Wertvorstellungen der Gesellschaft akzeptiert wird". Das *Restrisiko* ist das Risiko, das nach der Anwendung der jeweiligen Schutzmaßnahmen verbleibt.





Neben diesen Termini verwendet der Fachbericht 144 den Begriff der *Gefährdung* als Übersetzung des englischen Begriffs „hazard" und bezeichnet damit eine potenzielle Schadensquelle. Aus dem Begriff der Gefährdung werden drei weitere Begriffe abgeleitet: Die *Gefährdungssituation* ist ein Zustand, in dem Menschen, Güter oder die Umwelt einer oder mehreren Gefährdungen ausgesetzt sind; aus der Gefährdungssituation kann ein *Gefährdungsereignis*, das heißt ein Ereignis, das einen Schaden hervorrufen kann, hervorgehen. Resultiert aus einer Gefährdungssituation tatsächlich ein Schaden, wird von einem *Schadensereignis* gesprochen.

Die *Vorsorgesituationen* zeichnen sich dadurch aus, dass der kausale Schadensablauf hinsichtlich der im Raum stehenden Risiken nicht bewiesen, jedoch ein begründeter Verdacht eines Zusammenhangs mit gewissen Schadensabläufen gegeben ist. Die Beantwortung der Frage, welche Vorkehrungen zu treffen sind, unterliegt daher – vor allem politischen – Nützlichkeitserwägungen. Chancen und Risiken werden an dieser Stelle abgewogen und zu einer von Verhältnismäßigkeitsüberlegungen geprägten Lösung verarbeitet.

In den als *Meidungssituationen* bezeichneten Fällen ist weder eine Wirkursächlichkeit wissenschaftlich nachweisbar noch ein Wirkmodell für denkbare Schadensszenarien bekannt; die Annahme eines Risikos beruht vielmehr ausschließlich auf statistischen Auffälligkeiten (sogenannten Pseudorisiken). Dementsprechend beruht die Entscheidung, vom Einsatz einer Technologie Abstand zu nehmen, nicht auf einer wissenschaftlichen Beurteilung, sondern allein auf politischen Erwägungen.




Die *Risikobearbeitung* ist ein Vorgang, bei dem es ausschließlich um die Minderung von Risiken geht, ohne die Chancen des jeweiligen Produkts zu berücksichtigen. Beim *Risikomanagement* – damit befasst sich der Fachbericht 144 nicht näher – findet dagegen eine Abwägung zwischen Chancen einerseits sowie Risiken andererseits statt, die in ein mit subjektiven Maßstäben gewonnenes Ergebnis mündet.

5.2.2 VORGABEN FÜR DEN ABLAUF DER RISIKOBEARBEITUNG

5.2.2.1 SCHRITTE DER RISIKOBEARBEITUNG IN DER SICHERHEITSTECHNIK: RISIKOBEURTEILUNG UND RISIKOMINDERUNG

Die Risikobearbeitung im Bereich der Sicherheitstechnik besteht aus den Einzelschritten Risikobeurteilung und Risikominderung, die gegebenenfalls mehrfach wiederholt werden. Beide werden so lange vorgenommen, bis das verbleibende Risiko (*Restrisiko*) als vertretbar – und reziprok: das Produkt als sicher – zu bewerten ist.

Die *Risikobeurteilung* als erster prozeduraler Schritt der Risikobearbeitung setzt voraus, dass geeignete Risikodaten – also Informationen über vorhandene Gefährdungen, Art und Höhe möglicher Schäden sowie die Beziehung zwischen Ursache und Wirkung – vorhanden sind. Die Gewinnung der Risikodaten ist jedoch nicht unproblematisch: So





müssen insbesondere die Schutzbeiwerte, die ein Maß für eine Überdimensionierung bilden und damit zur Verringerung der Eintrittswahrscheinlichkeit eines Schadens beitragen, festgelegt werden. Die Festlegung von Schutzbeiwerten ist mit Unsicherheiten verbunden und erlegt daher den Konstrukteuren, den Normsetzern und den Normanwendern Verantwortung auf. Im Einzelnen können bei der Risikobeurteilung *drei Teilschritte* unterschieden werden: Identifizierung der Gefährdung, Risikoeinschätzung und Risikobewertung.

Zunächst müssen die Gefährdungen identifiziert werden. Hier bietet es sich an, den Lebenszyklus des Produkts und seine Einsatzetappen nachzuverfolgen. Bei der Ermittlung der möglichen Gefährdungen muss auch berücksichtigt werden, zu welchen Formen des Fehlgebrauchs es bei der Bedienung durch unkundige oder leichtfertige Nutzer kommen kann und welche Sondersituationen (zum Beispiel Stromausfall oder Versagen einzelner Teile des Produkts) auftreten können.

Im zweiten Teilschritt erfolgt die Risikoeinschätzung. Hier begegnet man – was auch der Fachbericht 144 darstellt – der Schwierigkeit, dass eine klare Einschätzung hinsichtlich der Bestimmungsgrößen des Risikos (Eintrittswahrscheinlichkeit und Schadensausmaß) häufig nur bedingt möglich ist. Eine Möglichkeit, sich zu behelfen, besteht darin, Klassen der Eintrittswahrscheinlichkeit (zum Beispiel fünf Klassen von „vernachlässigbar" bis „sehr wahrscheinlich") und des Schadensausmaßes (zum Beispiel drei Klassen von „kleine reversible Verletzungen" bis „irreversible schwere Verletzungen bis zum Tod") zu bilden. Dies erlaubt eine qualitative Bestimmung.




Auf der Basis dieser Informationen erfolgt im letzten Schritt die Risikobewertung. Grundlage dafür sind die Wertvorstellungen der Gesellschaft; zur Orientierung können in gewissem Umfang Risikovergleiche hilfreich sein. Die Risikobewertung muss oftmals generell getroffen werden, obwohl die Risikoeinschätzung sehr individuell geprägt ist. Die für die Akzeptanz maßgebliche innere Einstellung zu einem Risiko hängt stark davon ab, ob es freiwillig eingegangen wird und in welchem Umfang es beeinflusst werden kann.

Führt die Risikobewertung zu dem Ergebnis, dass das Risiko – noch – nicht vertretbar ist, schließt sich der zweite prozedurale Schritt an: die *Risikominderung*. Sie kann ebenfalls in *drei Teilschritte* untergliedert werden: sicherheitsbezogene Konstruktion, technische und ergänzende Schutzmaßnahmen sowie Benutzerhinweise.

Erstes Mittel der Wahl ist eine sicherheitsbezogene Konstruktion des Produkts. An dieser Stelle werden Gestaltung, insbesondere Form und Gewicht, und Werkstoffe relevant. Eine unter Sicherheitsaspekten getroffene Auswahl kann die Eintrittswahrscheinlichkeit von Schäden mindern und deren Ausmaß begrenzen.

Lassen sich durch derartige Maßnahmen keine ausreichenden Erfolge erzielen, müssen – im zweiten Teilschritt – technische und ergänzende Schutzmaßnahmen ergriffen werden. Klassische Beispiele hierfür sind trennende Schutzeinrichtungen (etwa Maschi-





nengehäuse und -abdeckung) und nichttrennende Schutzeinrichtungen (wie Verriegelungen). Diese Maßnahmen führen meist zu einer Minderung der Eintrittswahrscheinlichkeit, während sie das Ausmaß eines dennoch eintretenden Schadens unverändert lassen.

Haben beide Teilschritte das Risiko nicht ausreichend gemindert, muss die Sicherheit durch Benutzerhinweise gesteigert werden. Diese können am Produkt selbst angebracht oder in der Bedienungsanleitung enthalten sein. Die Verhaltensweisen, über die unterrichtet wird, erstrecken sich auf den gesamten Lebenszyklus von der Auslieferung bis zur Entsorgung. In den Benutzerhinweisen ist auch auf mögliche Formen der Fehlbedienung und deren Folgen sowie auf geeignete Schutzmaßnahmen einzugehen.

5.2.2.2 SCHRITTE DER RISIKOBEARBEITUNG IN DER VORSORGE: ORIENTIERUNG AM GRUNDSATZ DER VERHÄLTNISMÄSSIGKEIT

Für den durch einen begründeten Risikoverdacht gekennzeichneten Bereich der Vorsorge kann die Terminologie aus der Sicherheitstechnik grundsätzlich übernommen werden. Anders als dort, orientieren sich die zu ergreifenden Maßnahmen in erster Linie am *Verhältnismäßigkeitsgrundsatz*. Es findet somit im Hinblick auf die Risikominderung eine an wirtschaftlichen Überlegungen orientierte Kosten-Nutzen-Analyse statt. Die ökonomische Sicht gebietet, gewisse Risiken in Kauf zu nehmen, wenn ihre Beseitigung höhere Kosten verursacht als die Kompensation der Schäden. Der Zielkonflikt zwischen Sicherheit und Wirtschaftlichkeit wird in der Regel durch die einschlägigen technischen Normen entschieden. Eine bedeutende Grenze für das Maß des Aufwands, der zur Vorsorge zu betreiben ist, bildet der Stand der Technik.




An dieser Stelle ist zu berücksichtigen, dass die öffentliche Besorgnis bei den einzelnen Sachverhalten stark unterschiedlich ausgeprägt ist, obwohl aus fachlicher Sicht eine gleichartige Behandlung geboten erscheint. Da sich der Bereich der Vorsorge dadurch auszeichnet, dass die Ursache-Wirkungs-Beziehung nicht erforscht ist, lässt sich hier nicht mit Risikovergleichen arbeiten. Werden mehrere Vorsorgemaßnahmen ergriffen, sind diese aufeinander abzustimmen und mit früheren oder künftig zu erwartenden zu koordinieren. Wegen der Abhängigkeit der Vorsorgemaßnahmen von den jeweiligen wissenschaftlichen Erkenntnissen muss eine Veränderung des Erkenntnisstandes umgehend eine Anpassung der Maßnahmen nach sich ziehen.

Die fehlende wissenschaftliche Absicherung bewirkt im Vergleich zur Sicherheitstechnik einen größeren Spielraum für die Entscheidung, welche Maßnahmen ergriffen werden. Die vorwiegend politisch getroffene Entscheidung muss den individuellen und kollektiven Ansprüchen der Gesellschaft gerecht werden. Ob eine Entscheidung von den Bürgern akzeptiert wird, hängt nicht zuletzt vom Informationsstand der Öffentlichkeit ab.





5.2.2.3 MEIDUNG

Mit Meidung spricht der Fachbericht 144 Situationen an, in denen objektivierbare Risiken nicht gegeben sind, aber gleichwohl Maßnahmen ergriffen werden, die von einzelnen Geboten und Verboten bis zum teilweisen oder vollständigen Verzicht reichen können. Diese sind dann ausschließlich politisch motiviert und sollen Besorgnisse in der Bevölkerung abbauen.

5.3 ZU BEWÄLTIGENDE ZIELKONFLIKTE

Ohne diese explizit zu benennen, ist der Fachbericht 144 um angemessene Lösungsverfahren für verschiedene Zielkonflikte bemüht. Die beiden wichtigsten Zielkonflikte sollen hier deshalb nochmals kurz aufgegriffen werden.

5.3.1 RISIKEN GEGEN CHANCEN (RISIKOMANAGEMENT)





Mit seiner Differenzierung zwischen Risikomanagement (risk management) und Risikobearbeitung (risk treatment) arbeitet der Fachbericht 144 ein wesentliches Unterscheidungsmerkmal zweier Abwägungsverfahren heraus. Die Risikobearbeitung beschränkt sich im Bereich der Sicherheitstechnik allein auf die Betrachtung der in Rede stehenden Risiken. Diese sind so lange zu mindern, bis das Restrisiko nicht größer ist als das maximal vertretbare Risiko, denn auch noch so große Chancen können den Anspruch der Bürger auf Sicherheit nicht kompensieren und dürfen daher überhaupt nicht berücksichtigt werden. Das Risikomanagement, das Chancen und Risiken gegeneinander abwägt, wird für den Bereich der Sicherheitstechnik vor allem deshalb abgelehnt, weil es durch „diffizile, subjektive und angreifbare Güterabwägungen" gekennzeichnet ist. Lediglich im Bereich der Vorsorge wird ihm ein originärer Anwendungsbereich eingeräumt. Dort werden die Zielkonflikte, zum Beispiel zwischen Sicherheit und Wirtschaftlichkeit, durch die technischen Normen entschieden. Dabei bildet der Stand der Technik eine bedeutende Grenze für das Maß des Aufwands, der als Vorsorge zu betreiben ist. Bei der Gefahrenabwehr kommt dem Stand der Technik diese Bedeutung hingegen nicht zu, da Gefahren den Betroffenen niemals zugemutet werden können.

5.3.2 RISIKEN GEGEN KOSTEN

Anders als für den Bereich der Sicherheitstechnik festgestellt, ergibt sich im Bereich der Vorsorge (also unterhalb des maximal vertretbaren Risikos) ein Regelungsspielraum. Hier geht es letztlich um die Frage, wie weit man durch die zu treffende Regelung „auf der sicheren Seite" sein will. Da für geeignete Vorsorgemaßnahmen keine feste Grenze zu ermitteln ist, kommt es letztlich auf eine Abwägung von Kosten und Chancen der Risikominderung an, die vor allem von Fragen der Verhältnismäßigkeit bestimmt wird.





5.4 VERGLEICH MIT DER TERMINOLOGIE DER RECHTSORDNUNG:

Die Steuerungsmechanismen, die die Rechtsordnung zur Gewährleistung der technischen Sicherheit vorsieht, sind heterogen. Idealtypisch lassen sich drei Varianten bilden: die Selbstregulierung durch die unmittelbar Betroffenen, die europäische und nationale imperative Regulierung sowie – als Zwischenform – die kooperative Steuerung EU/Staat – Unternehmen/Privatpersonen. Dieser Zwischenform kommt insbesondere durch Einbeziehung der technischen Normung mit deren Beschaffenheits- und Verhaltensanforderungen größte praktische Bedeutung zu.

Mit Blick auf die praktische Relevanz soll im Folgenden beispielhaft zunächst auf den Sprachgebrauch des Bundes-Immissionsschutzgesetzes (BImSchG) und der darauf gestützten Störfall-Verordnung eingegangen werden, die nicht nur das Umweltrecht prägen, sondern auch die Gewährleistung der Sicherheit technischer Anlagen bestimmen, bevor die im Fachbericht 144 vorgenommene terminologische Differenzierung daraufhin untersucht wird, ob sie mit dem juristischen Sprachgebrauch in Einklang zu bringen ist. Daran anschließend, wird der Sprachgebrauch des Geräte- und Produktsicherheitsgesetzes (GPSG) und des Produkthaftungsgesetzes (ProdHaftG) beschrieben und mit dem des Fachberichts 144 verglichen.

5.4.1 BUNDES-IMMISSIONSSCHUTZGESETZ UND STÖRFALL-VERORDNUNG




Die vom DIN-Fachbericht 144 vorgenommene Differenzierung zwischen der Risikobearbeitung in der Sicherheitstechnik und dem Risikomanagement, das eine Abwägung von Risiken und Chancen umfasst, entspricht der Differenzierung zwischen dem Schutz- und dem Vorsorgeprinzip, die der Gesetzgeber in den meisten Gesetzen des Sicherheitsrechts einschließlich des Umweltrechts (zum Beispiel im BImSchG) angelegt hat: § 5 Abs. 1 Nr. 1 BImSchG verwirklicht das Schutzprinzip, indem gefordert wird, dass bei der Errichtung und dem Betrieb der Anlagen schädliche Umwelteinwirkungen, sonstige Gefahren und erhebliche Nachteile nicht hervorgerufen werden dürfen. Nach dieser – strikten – Vorgabe haben die Chancen der Technik oder die Wirtschaftlichkeit des Schadensvermeidungsaufwands keinen Einfluss auf das Ergebnis, weil es an dieser Stelle darum geht, Schäden abzuwehren, deren Hinnahme für Nachbarn und andere stets unzumutbar ist. Der – weitergehende – Vorsorgegedanke wird in § 5 Abs. 1 Nr. 2 BImSchG umgesetzt. Diese Bestimmung nimmt auf den Stand der Technik Bezug. Dieser ist, wie sich aus dem Anhang zu § 3 Abs. 6 BImSchG ergibt, „unter Berücksichtigung der Verhältnismäßigkeit zwischen Aufwand und Nutzen" zu bestimmen. Hierbei führt der Anhang zu § 3 Abs. 6 BImSchG eine Vielzahl von – nicht abschließend gemeinten – Einzelkriterien an, so etwa, ob der Einsatz weniger gefährlicher Stoffe möglich ist (Nr. 2), ob vergleichbare Techniken bereits im Betrieb erprobt sind (Nr. 4) und welche Zeit für die Einführung einer



besseren Technologie notwendig ist (Nr. 8). Mit Nr. 5 – Fortschritte in den wissenschaftlichen Erkenntnissen – geht der Katalog über den hergebrachten Begriff des Standes der Technik sogar hinaus. In ähnlicher Weise gibt der Fachbericht 144, der in diesem Zusammenhang die juristische Terminologie aufnimmt, bei den Grundsätzen für die Vorsorge ausdrücklich vor, die „Vorsorgemaßnahmen den Erkenntnissen der Wissenschaft" anzupassen.

Um den Stand der Technik für einzelne Anlagenarten oder für die Reaktion auf bestimmte Szenarien abzubilden, sieht das BImSchG den Erlass von Rechtsverordnungen und Verwaltungsvorschriften (vgl. § 48 BImSchG) vor. Doch auch diese geben oftmals den Stand der Technik nicht selbst wieder, sondern verweisen – direkt oder indirekt – auf technische Normen zum Beispiel des DIN.

Ein Beispiel für eine solche Rechtsverordnung ist die 12. BImSchV, die sogenannte Störfall-Verordnung (Störfall-VO), die eine europäische Richtlinie umsetzt. Die Störfall-VO befasst sich mit gefährlichen Stoffen und dient auf diese Weise in erster Linie der Anlagensicherheit. Bislang existiert noch keine gültige Ausführungsvorschrift der Bundesregierung zur Störfall-VO, da die von der Bundesregierung am 10. Dezember 2003 beschlossene „Allgemeine Verwaltungsvorschrift zur Störfall-Verordnung" (StörfallVwV) im Bundesrat keine Mehrheit gefunden hat. Ihr Inhalt kann aber als Auslegungshilfe herangezogen werden. Das Bundesministerium für Umweltschutz, Naturschutz und Reaktorsicherheit hat die vom Bundesrat abgelehnte Verwaltungsvorschrift überarbeitet und stellt sie als Vollzugshilfe zur Störfall-VO den Länderbehörden und der Wirtschaft zur Verfügung. Diese Vollzugshilfe nimmt wiederum zum Beispiel Bezug auf Normen des DIN sowie des VDI/VDE, aus denen sich dann die konkreten Anforderungen ergeben.




Aus juristischer Sicht ist die im Fachbericht 144 vorgenommene strikte Trennung der Risikobearbeitung in der Sicherheitstechnik vom Risikomanagement in der Vorsorge positiv zu bewerten. Allerdings ist der Begriff „Risikomanagement" im juristischen Sprachgebrauch unüblich und im Übrigen auch wenig aussage- und unterscheidungskräftig. Vorzuziehen wäre daher – um die Berücksichtigung der Chancen deutlich zu machen – der Begriff „Risiko-Chancen-Management".

Die Terminologie des Fachberichts 144 im Bereich Gefahr/Sicherheit/Risiko deckt sich weitgehend mit dem juristischen Sprachgebrauch. Nach dem juristischen Gefahrenbegriff, wie er insbesondere im Polizei- und Ordnungsrecht anzutreffen ist, bezeichnet Gefahr einen Zustand, bei dem mit hinreichender Wahrscheinlichkeit der Eintritt eines nicht unerheblichen Schadens für ein geschütztes Rechtsgut zu erwarten ist. Sachlich stimmt damit die Definition des vertretbaren Risikos überein, da dessen Gegenteil – das unvertretbare Risiko – den Zustand der Gefahr ausmacht und das Risiko selbst sich aus dem Produkt aus Eintrittswahrscheinlichkeit und erwartetem Schaden ergibt. Im juristischen Bereich steht lediglich „negativ" der zu vermeidende Schaden im Blickfeld, während im technischen Bereich „positiv" die herzustellende Sicherheit betrachtet wird.





Über die genannten Termini hinaus findet sich im Fachbericht 144 der Begriff der „Gefährdung“ als einer der Gefahr vorgelagerten Risikostufe, also eine potenzielle Schadensquelle. Aus der Gefährdung wird eine „Gefährdungssituation“, sobald eine Einwirkung auf Menschen und Rechtsgüter möglich wird. Erst dann wird aus dieser durch Hinzutreten eines Gefährdungsereignisses eine Gefahr im eigentlichen Sinn (das heißt, das Risiko nimmt ein unvertretbares Maß an). Im juristischen Sprachgebrauch findet sich zu diesen Begriffen jeweils kaum eine Entsprechung. Dort kommt es – zumeist für die Frage, ob ein Hoheitsträger durch eine Einzelfallanordnung eingreifen darf – regelmäßig nur darauf an, ob ein bestimmter Zustand jeweils für sich betrachtet bereits eine Gefahr darstellt oder nicht, insbesondere, ob der Schadenseintritt schon als hinreichend wahrscheinlich zu bewerten ist. Verbreitet ist dabei die Unterscheidung zwischen einer abstrakten (allgemeinen) und einer konkreten – also nach Zeit und Ort bestimmbaren – Gefahr. Ist ein Sachverhalt zunächst ungefährlich und entwickelt sich erst durch Hinzutreten eines weiteren Ereignisses zur Gefahr, so wird von einer latenten Gefahr gesprochen (ein Beispiel ist das Brandrisiko eines Reetdaches). Diesem Begriff dürfte die Gefährdung im Sinne des Fachberichts 144 weitgehend entsprechen.

5.4.2 GERÄTE- UND PRODUKTSICHERHEITSGESETZ





Das Geräte- und Produktsicherheitsgesetz (GPSG) erfasst technische Arbeitsmittel und Verbraucherprodukte und hat damit einen ausgesprochen großen Anwendungsbereich. Wie dem Bundes-Immissionsschutzgesetz (BImSchG) liegt auch dem GPSG eine – der Differenzierung zwischen Risikobearbeitung und Risikomanagement entsprechende – Unterscheidung zwischen dem Schutz- und dem Vorsorgeprinzip zugrunde: Existiert für das Produkt eine gemäß § 3 Abs. 1 GPSG erlassene Rechtsverordnung (so zum Beispiel zu Druckbehältern, Maschinen und Aufzügen), so verlangt § 4 Abs. 1 GPSG, dass das Produkt nur dann in den Verkehr gebracht werden darf, wenn es den in der Rechtsverordnung nach § 3 Abs. 1 GPSG festgelegten Anforderungen an Sicherheit und Gesundheit und den sonstigen Voraussetzungen für sein Inverkehrbringen entspricht sowie Sicherheit und Gesundheit der Verwender oder Dritter oder sonstige in den Rechtsverordnungen nach § 3 Abs. 1 GPSG aufgeführte Rechtsgüter bei bestimmungsgemäßer Verwendung oder vorhersehbarer Fehlanwendung nicht gefährdet werden. Hierdurch wird das Schutzprinzip verwirklicht. Chancen der Technik sowie Wirtschaftlichkeitserwägungen bleiben dabei unberücksichtigt.

Als Ausdruck des „New Approach“ stellt § 4 Abs. 1 S. 2 GPSG die Vermutung auf, dass ein normgemäß hergestelltes Produkt den betreffenden Anforderungen an Sicherheit und Gesundheit genügt, sofern es sich bei der technischen Norm um eine sogenannte harmonisierte Norm handelt. Existiert keine Rechtsverordnung im Sinne von § 4 Abs. 1 GPSG, so darf gemäß § 4 Abs. 2 GPSG ein Produkt nur dann in den Verkehr gebracht werden, wenn es so beschaffen ist, dass bei bestimmungsgemäßer



Verwendung oder vorhersehbarer Fehlanwendung Sicherheit und Gesundheit von Verwendern oder Dritten nicht gefährdet werden. Auch diese Regelung ist an sich Ausdruck des Schutzprinzips. Bei der Beurteilung, ob ein Produkt den Anforderungen des § 4 Abs. 2 GPSG entspricht, können jedoch Normen und andere technische Spezifikationen zugrunde gelegt werden (vgl. § 4 Abs. 2 S. 3 GPSG). Auf diese Weise kommt das Vorsorgeprinzip zum Tragen, indem im Bereich der Normung Zielkonflikte zum Beispiel zwischen Sicherheit und Wirtschaftlichkeit entschieden werden. Da bei der technischen Normung aus Praktikabilitätsgründen oft nicht scharf zwischen Gefährdungs- und Vorsorgesituationen unterschieden wird, muss gegebenenfalls kritisch geprüft werden, ob mit dem Abwägungsvorgang auch der Bereich der Gefahr erfasst sein soll und damit die Vermutungswirkung nicht eingreifen kann. Um solche Situationen zu vermeiden, sollten sich technische Normen möglichst nicht mit Vorsorgesituationen befassen, sondern dies zumindest in Bezug auf die Festlegung von Grenzwerten dem Gesetzgeber überlassen.




Für Verbraucherprodukte finden sich in § 5 Abs. 1 Nr. 1 a) – c) GPSG besondere Ausprägungen des Vorsorgegrundsatzes: So ist gemäß § 5 Abs. 1 Nr. 1a) GPSG sicherzustellen, dass der Verwender die zur Schadensvermeidung notwendigen Informationen erhält. Gemäß § 5 Abs. 1 Nr. 1c) GPSG hat der Hersteller durch interne Organisation (Risikomanagement) zur Vermeidung von Gefahren Vorkehrungen zu treffen, die an die Eigenschaften des von ihm in den Verkehr gebrachten Verbraucherprodukts angepasst sind. Das Spektrum reicht von der Warnung über die Rücknahme bis zum Rückruf.

Als *Ergebnis* lässt sich festhalten: Auch im GPSG findet sich die Unterscheidung von Schutzprinzip und Vorsorgeprinzip, der der Fachbericht 144 in seiner Unterscheidung von Risikobearbeitung und Risikomanagement folgt.

5.4.3 PRODUKTHAFTUNGSGESETZ

Das Produkthaftungsgesetz (ProdHaftG) ist mit der darin insbesondere für Hersteller vorgesehenen verschuldensunabhängigen Haftung ein zentrales juristisches Steuerungsinstrument für eine Vielzahl von Produkten. Auch in seinem Anwendungsbereich kann zumindest im Ansatz zwischen dem Schutz- und Vorsorgeprinzip differenziert werden. Dabei kommt dem Schutzprinzip insoweit eine überragende Bedeutung zu. Eine zentrale Rolle spielt der Fehlerbegriff des § 3 ProdHaftG. Gemäß § 3 Abs. 1 ProdHaftG ist ein Produkt *fehlerhaft*, wenn es nicht die Sicherheit bietet, die unter Berücksichtigung aller Umstände, insbesondere seiner Darbietung, des Gebrauchs, mit dem billigerweise gerechnet werden kann, sowie des Zeitpunkts, in dem es in den Verkehr gebracht wurde, berechtigterweise erwartet werden kann. Im Hinblick auf den Gebrauch des Produkts gilt es zu berücksichtigen, dass dieser grundsätzlich nicht nur die bestimmungsgemäße Verwendung, sondern auch den vorhersehbaren Fehlgebrauch umfasst. Es bedarf insoweit einer Abgrenzung zwischen einem (noch) haftungsrelevanten Fehlgebrauch und einem der Risikosphäre des Herstellers nicht mehr zurechenbaren Missbrauch des





Produkts. Die maßgeblichen Sicherheitserwartungen sollen nach vielfach vertretener Auffassung anhand des Horizonts der durch die fehlende Produktsicherheit betroffenen Allgemeinheit bestimmt und beurteilt werden. Teilweise wird auch auf das Verständnis eines verständigen Verbrauchers abgestellt. Unter Ausblendung einiger Detailfragen ist insoweit nach allgemeiner Auffassung eine objektive Betrachtungsweise geboten. Einzubeziehen sind dabei nicht nur die berechtigten Sicherheitserwartungen der Produktnutzer selbst, sondern auch diejenigen außenstehender Dritter (sogenannter „innocent bystander").

Die Feststellung des Vorliegens eines Produktfehlers orientiert sich demnach grundsätzlich an den im Hinblick auf die Risikobearbeitung dargestellten Erwägungen. Die Perspektive ist jedoch insoweit eine etwas andere, als das Haftungsregime des ProdHaftG reaktiv und retrospektiv auf den Eintritt eines Schadens abstellt. Das Nichtvorliegen einer hinreichenden Risikobearbeitung wird als Ansatzpunkt für eine Haftung für Personen- und Vermögensschäden genommen. Es gilt demnach auch für das Haftungsrecht zu klären, wie sicher sicher genug ist. Die Abgrenzung zur Vorsorge ist allerdings im Bereich der Haftung nicht vergleichbar konsequent realisiert. So können nach nahezu unbestrittener Auffassung – anders als im Bereich der Risikobearbeitung – auch wirtschaftliche Erwägungen miteinbezogen werden. Insbesondere soll dem Preis des Produkts eine erhebliche Bedeutung zukommen können. Eine Schranke, die nicht unterschritten werden darf, bildet allerdings die sogenannte Basissicherheit. Zumindest elementarsten Sicherheitsanforderungen muss das Produkt unabhängig von einem unter Umständen niedrigen Preis genügen.





Besonderheiten können sich bei Vorliegen zwingender gesetzlicher Vorgaben ergeben. Sofern dem Hersteller der Nachweis gelingt, diese vollumfänglich beachtet zu haben, scheidet gemäß § 1 Abs. 2 Nr. 4 ProdHaftG eine Haftung aus. Anders zu beurteilen ist dies im Hinblick auf die Einhaltung technischer Normen, die aus Sicht des Haftungsrechts zumeist nicht mehr als einen unabdingbaren Mindeststandard beschreiben. Insoweit kommt das Vorsorgeprinzip – anders als etwa im Bereich der Produktsicherheit – nicht zum Tragen. Als eine weitere wichtige Haftungsausschlussnorm ist in diesem Zusammenhang § 1 Abs. 2 Nr. 5 ProdHaftG zu nennen. Diese Norm stellt im Zusammenwirken mit § 3 Abs. 2 ProdHaftG klar, dass eine Haftung ausscheidet, soweit der Fehler nach dem Stand der Wissenschaft und Technik in dem Zeitpunkt, in dem der Hersteller das Produkt in den Verkehr brachte, nicht erkannt werden konnte (sogenannter *Entwicklungsfehler*). Die Erkennbarkeit richtet sich dabei wiederum nicht nach individuellen, sondern vielmehr nach rein objektiven Maßstäben. Von einem derartigen Entwicklungsfehler sind sogenannte Entwicklungslücken abzugrenzen, bei denen der Hersteller den Fehler zwar erkennen, ihn jedoch nach dem Stand der Wissenschaft und Technik nicht verhindern konnte. Bei Vorliegen einer Entwicklungslücke hat ein Inverkehrbringen gegebenenfalls zu unterbleiben. Falls sich der Hersteller trotz erkann-





ter, technisch nicht zu vermeidender Produktfehler für ein Inverkehrbringen entscheidet, folgt daraus eine Haftung des Herstellers nach dem ProdHaftG. Im Ergebnis verlangt auch das ProdHaftG vom Hersteller grundsätzlich eine hinreichende Risikobearbeitung. Eine Haftung scheidet nur dann aus, wenn der Produktfehler objektiv zum Zeitpunkt des Inverkehrbringens nicht erkannt werden konnte.

5.5 ZUSAMMENFASSUNG

Der Verständigung zwischen den Disziplinen Technik und Recht kommt deshalb besondere Bedeutung zu, weil wesentliche Entscheidungen – insbesondere über die Zulassung technischer Produkte, die Haftung für fehlerhafte Produkte und gegebenenfalls die strafrechtliche Verantwortlichkeit – auf rechtlichen Vorgaben beruhen. Sollen insbesondere negative wirtschaftliche Konsequenzen vermieden werden, müssen Entwicklung und Anwendung von Technik diese rechtlichen Vorgaben im Blick haben.

Die technische Normung verbindet Technik und Recht an ihren Nahtstellen. Diese Verbindung erfolgt insbesondere durch Konkretisierung der zumeist durch unbestimmte Rechtsbegriffe (zum Beispiel „Stand der Technik“, „anerkannte Regeln der Technik“) oder allgemeine Zielvorgaben (zum Beispiel „keine Gefährdung der Sicherheit“, „Vermeidung von Gefahren und erheblichen Nachteilen“) formulierten rechtlichen Anforderungen. Dieser Konkretisierung kann nur dann Erfolg beschieden sein, wenn in terminologischer Hinsicht keine relevanten Diskrepanzen bestehen. Der vom DIN im Jahre 2005 herausgegebene Fachbericht 144 „Sicherheit, Vorsorge und Meidung in der Technik“ definiert Risiko als Kombination aus der Wahrscheinlichkeit des Schadenseintritts und des Schadensausmaßes unter Ausblendung etwaiger Chancen. Das nach den gültigen Wertvorstellungen der Gesellschaft akzeptierte Risiko entscheidet über dessen Vertretbarkeit und grenzt das sogenannte Restrisiko ab. Die Begriffe Gefahr und Sicherheit werden durch die Anwesenheit bzw. Abwesenheit eines unvertretbaren Risikos umschrieben. Die Risikobearbeitung setzt sich aus den beiden prozeduralen Schritten der Risikobeurteilung und der Risikominderung zusammen. Betrachtet werden allein die Risiken. Eine Kompensation durch Chancen (verstanden als Oberbegriff für Vorteile, Nutzen und andere positive Effekte sowie Erwartungen) findet nicht statt. Anders erfolgt die Betrachtung im sogenannten Vorsorgebereich des Restrisikos. Hier kommt es auf eine Abwägung von Kosten und Chancen der Risikominderung nach dem Grundsatz der Verhältnismäßigkeit an.




Der Vergleich mit den gesetzlichen Regelungen des Bundes-Immissionsschutzgesetzes (BImSchG), der Störfall-VO, des Geräte- und Produktsicherheitsgesetzes (GPSG) und des Produkthaftungsgesetzes (ProdHaftG) zeigt, dass der Fachbericht 144 im Ergebnis dem juristischen Verständnis sehr nahe kommt und damit eine wertvolle Verständigungsbrücke zwischen Technik und Recht bildet. Ein Endpunkt terminologischer Klar-





heit ist damit noch nicht erreicht. Wünschenswert wäre eine alle Bereiche technischen Risikos (zum Beispiel auch Kernergie und Gentechnik) umfassende Untersuchung, die sich auch auf die internationale Ebene erstreckt.

5.6 LITERATUR

DIN 2005
DIN Deutsches Institut für Normung e. V. (Hrsg.): DIN-Fachbericht 144: Sicherheit, Vorsorge und Meidung in der Technik, Berlin: Beuth Verlag, 2005.

DIN 2008
DIN Deutsches Institut für Normung e. V. (Hrsg.): DIN 820-120: Leitfaden für die Aufnahme von Sicherheitsaspekten in Normen, (ISO/IEC-Guide 51: 1999), Berlin: Beuth Verlag, 2008.

Dietz/Regenfus 2006
Dietz, F./Regenfus, T.: „Risiko und technische Normung im Spannungsfeld von Recht und Technik." In: Vieweg, K. (Hrsg.): Risiko – Recht – Verantwortung, Köln, Berlin, Bonn, München: Carl Heymanns Verlag, 2006, S. 403-429.




Falke 2006
Falke, J.: „Management von Risiken technischer Produkte im Rahmen der Neuen Konzeption zur technischen Harmonisierung und Normung." In: Vieweg, K. (Hrsg.): Risiko – Recht – Verantwortung, Köln, Berlin, Bonn, München: Carl Heymanns Verlag, 2006.

Hosemann 2007
Hosemann, G.: „Risikobeurteilung zur Konkretisierung staatlicher Vorschriften." In: etz (2007), Nr. 12, S. 76–81.

Lukes/Feldmann/Knüppel 1980
Lukes, R./Feldmann, F.-J./Knüppel, H.-C.: „Länderbericht Bundesrepublik Deutschland." In: Lukes, R. (Hrsg.): Gefahren und Gefahrenbeurteilungen im Recht, Teil II, Köln, Berlin, Bonn, München: Carl Heymanns Verlag, 1980, S. 71-207.

Marburger 1994
Marburger, P.: „Technische Regeln." In: Kimminich, O./Frhr. v. Lersner, H./Storm, P.-C. (Hrsg.): Handbuch des Umweltrechts, Berlin: Schmidt Verlag, 1994, Sp. 2045 ff.



Reich 1989
Reich, A.: Gefahr – Risiko – Restrisiko, Düsseldorf: Werner Verlag, 1989.

Renn 2002
Renn, O.: „Die subjektive Wahrnehmung technischer Risiken." In: Förderkreis des Fachbereichs Elektrotechnik (Hrsg.): Risiko Kernkraft, Mobilfunk, BSE, Terror, Straßenverkehr ... Unser Umgang mit der Angst, (7. Fuldaer Elektrotechnik-Kolloquium, Elektronik-Fachberichte 7), Fulda, 2002, S. 12-23 – Tagungsband.

VDI 2007
Verein Deutscher Ingenieure (VDI): Qualitätsmerkmal „Technische Sicherheit". Eine Denkschrift des Vereins Deutscher Ingenieure (2007). URL: http://www.vdi.de/fileadmin/vdi_de/redakteur_dateien/rili_dateien/Qualitaetsmerkmal_Technische_Sicherheit.pdf [Stand: 22.07.2009].



Vieweg 1980
Vieweg, K.: „Gesamtdiskussion." In: Lukes, R. (Hrsg.): Gefahren und Gefahrenbeurteilungen im Recht, Teil I, Köln, Berlin, Bonn, München: Carl Heymanns Verlag, 1980, S. 177-201.



Vieweg 1993
Vieweg, K.: „Recht und Risiko." In: GSF-Forschungszentrum für Umwelt und Gesundheit (Hrsg.): mensch + umwelt, 8. Aufl., Neuherberg, 1993, S. 47-52.

Vieweg 2003
Vieweg, K.: „Produkthaftung." In: Schulte, M. (Hrsg.): Handbuch des Technikrechts, Berlin: Springer Verlag, 2003, S. 355 ff.



> RISIKOFORSCHUNG UND SICHERHEITSKULTUREN








1 INTERDISZIPLINÄRE RISIKO- UND SICHERHEITS-FORSCHUNG

ANNELY ROTHKEGEL/GERHARD BANSE/ORTWIN RENN

1.1 „RISIKO" UND „SICHERHEIT": ZWEI SCHILLERNDE BEGRIFFE

Risiko beruht auf dem Gegensatz zwischen Notwendigkeit und Möglichkeit.[1] Erst wenn die Zukunft als von Menschen zumindest teilweise gestaltbar angesehen wird, ist es möglich, potenzielle Gefahren zu vermeiden oder deren Konsequenzen zu mildern.[2] Das Denken in Kategorien von „Risiko" (und auch „Chance") setzt in Maßen Gestaltbarkeit der Zukunft und damit Vermeidbarkeit von tragischen Ereignissen durch Vorsorge voraus. Die Vorhersage möglicher Gefahren ist darauf angewiesen, dass kausale Beziehungen zwischen dem Verursacher der Gefahr und den Konsequenzen gezogen werden können. Diese Kausalbeziehungen können systematisch, anekdotisch, religiös oder magisch sein.[3] Da die Konsequenzen unerwünscht sind, umfasst „Risiko" immer auch ein normatives Konzept. Die Gesellschaft ist angehalten, Risiken zu vermeiden, zu verringern oder zumindest zu kontrollieren. Mit Zunahme der technischen Gefahrenpotenziale und der kulturellen Einverleibung von externen Gefahren in berechenbare Risikokalküle wächst der Bedarf an Risiko-Wissenschaft und -Management.[4]

„Risiken" bezeichnen also Möglichkeiten von zukünftigen Handlungsfolgen, die im Urteil der überwiegenden Zahl der Menschen als unerwünscht gelten. Risikokonzepte in den unterschiedlichen Disziplinen unterscheiden sich nach der Art und Weise, wie diese Handlungsfolgen erfasst und bewertet werden.[5] Die Menschheit ist dabei einer kaum überschaubaren Vielfalt von Risiken ausgesetzt. Ein Teil dieser Risiken ist mit natürlichen Abläufen und Ereignissen verbunden, andere sind aufgrund von menschlichen Aktivitäten entstanden oder verstärkt worden. Das grundsätzliche Dilemma besteht darin, dass alle menschlichen Aktivitäten mehr oder weniger große Potenziale für unbeabsichtigte Nebenwirkungen umfassen, gleichzeitig aber die Bedürfnisse des Menschen ohne derartige Aktivitäten nicht zu erfüllen sind. *Risiken einzugehen ist also ein notwendiger Bestandteil menschlichen Verhaltens* und damit erst die Voraussetzung für wirtschaftliche und soziale Entwicklung. Gleichzeitig ist aber eine Strategie der Risikoanhäufung für eine Gesellschaft existenzgefährdend: Es gilt daher, einen Mittelweg zwischen Chancenwahrnehmung und Risikobegrenzung zu finden.

---

1 Markowitz 1990, S. 385 sowie Jaeger et al. 2001.
2 Ewald 1993, S. 220.
3 Douglas 1966; Wiedemann 1993, S. 64.
4 Beck 1986, S. 36 ff.; Renn et al. 2007.
5 Banse 1996.





Wird ein Risiko als tolerierbar für eine Gesellschaft, das heißt auch für diejenigen als zumutbar bewertet, die selbst nicht an der Entscheidung mitwirken konnten, sprechen wir von „Sicherheit". Was sicher und was unsicher ist, kann also unter einem stochastischen Blickwinkel nicht als eine Ja-Nein-Entscheidung, sondern nur als eine analoge Graduierung von „mehr oder weniger sicher" aufgefasst werden. Als „sicher" bezeichnet man einen Zustand, bei dem das verbleibende Risiko als für alle tolerierbar angesehen wird. Die Sicherheit technischer Handlungsvollzüge und technischer Hervorbringungen als weitgehender Ausschluss oder als bewusstes Handling von (möglichen) stochastisch zu messenden Gefährdungen für „Schutzgüter" nimmt in den handlungsleitenden Wertvorstellungen technischer Welterzeugung einen herausragenden Platz ein.

1.2 SICHERHEIT IM SPIEGEL DER LINGUISTIK

Begriffe wie „Risiko", „Gefahr", „Gefährdung" oder „Sicherheit" werden in der Literatur sehr unterschiedlich definiert und konzeptualisiert. Bei einer Untersuchung des International Risk Governance Councils (IRGC) wurden insgesamt 46 Terminologien zu „Risiko" und „Sicherheit" unter die Lupe genommen und analysiert.[6] Dabei stellte sich heraus, dass selbst innerhalb eines Dokuments, erst recht aber zwischen offiziellen Dokumenten, erhebliche Bedeutungsunterschiede bei identischen Begriffen auftraten. Diese Vielfalt der Begriffsbedeutungen ist gerade im Bereich von Risiko und Sicherheit problematisch. Denn bei der Ausgestaltung von Sicherheitstechnik geht es um Leben und Tod. Die Wirksamkeit dieser Technik darf nicht von möglichen Missverständnissen über die Bedeutung von Begriffen wie „Risiko" und „Sicherheit" abhängig gemacht werden. Wie unterschiedliche Bedeutungen von Begriffen entstehen und wie sie durch Kommunikation verbreitet, aber auch verändert werden, ist ein Forschungsgegenstand der Linguistik.



Der Sprachgebrauch fungiert als Indikator für die Denkmodelle, die die Fach- und Sachkommunikation bestimmen.[7] Beziehen sich die Kommunikationspartner – bemerkt oder unbemerkt – auf unterschiedliche Wissensmodelle zum gleichen Thema, weil sie aus verschiedenen Disziplinen oder Kulturen kommen, entsteht ein Kommunikationsrisiko des Miss- oder Nicht-Verstehens. Inhalte und Ziele der Kommunikation wie Mitteilung, Verständigung oder Warnung sind möglicherweise intransparent. Das Kommunikationsrisiko ist besonders groß in der Experten-Nichtexperten-Kommunikation, die dadurch gekennzeichnet ist, dass die Beteiligten unterschiedliche Denkmodelle einbringen (disziplinäre theoretische Modelle, Konventionen und Gewohnheiten der Branche als Best Practice sowie Normen, Alltagsmodelle). Mit Bezug zur Mensch-Technik-Interaktion sind solche Kommunikationsrisiken inakzeptabel. Hier ist empirische Forschung gefragt:

6 IRGC 2005.
7 Rothkegel 2000; Rothkegel 2008.





Welche Sicherheitsmodelle prägen welche Kommunikationsszenarien (mit Parametern wie unter anderem Beteiligte, Themen, Intentionen, Text- und Dialogformen, Ort, Zeit, Medium) und umgekehrt? Welche Art von Sicherheit wird in welchen Kontexten versprochen, was sind die Gelingensbedingungen für diese Versprechen? In welchen Konstellationen geht es um Mitteilungen, Empfehlungen und Warnungen oder Drohungen? Welchen Stellenwert haben dabei Begriffe wie „Risiko" (Eintrittswahrscheinlichkeit und Schadensschwere), „Gefahr" (Gefahrenpotenzial, Gefahrenquelle, Gefährdung), „Schutz" (Schutzobjekt, Personen- und Objektschutz) und „Schaden" (Schadensereignis, Schadensschwere, Schadensziel)? Es tauchen Fragen nach den (historisch gewachsenen und veränderbaren) Spezifikationen auf: In welchem Modellen überlappen sich „Safety" und „Security", die gleichzeitig als Schlüsselbegriffe gelten, und welche Modelle sind produktiv für Paarbegriffe wie „aktive" und „passive Sicherheit" (vgl. zum Beispiel Risikomodell, Partnermodell)?

Begriffliche Systematiken, die ihrerseits aus Systematiken entwickelt werden, sind hilfreich als Einstieg, bilden aber letztlich nicht die Problematik und mögliche Lösungswege ab.[8] Empirische Forschung im Rahmen der Sicherheitskommunikation bedeutet Analyse und Bestandsaufnahme von Kommunikationsstrategien in authentischen Texten und Dialogen. Die kommunizierten Sicherheitsmodelle zusammen mit den sicherheitsrelevanten Kommunikationshandlungen bilden ein Inventar, das Sicherheitskulturen abbildet (vgl. Rothkegels Beitrag „Sicherheitsmodelle und Kommunikationsrisiko" in diesem Band). Als methodischen Zugriff bieten sich Verfahren der semantischen und pragmatischen Textanalyse an. Ziel ist die Dokumentation des analysierten Inventars in Form eines Thesaurus im webbasierten und interaktiv zugänglichen Wiki-Format.



Der linguistische Ansatz fokussiert gezielt auf die Soft Factors im Rahmen der Sicherheitskommunikation. Kommunikation bildet eine Brücke zwischen Technikentwicklung und Techniknutzung. Dabei kann es auch geschehen, dass die Techniknutzer als Akteure in einer veränderten Perspektive erscheinen. Dies gilt insbesondere für die Sicherheitskommunikation mit Bezug zur Mensch-Technik-Interaktion.[9] Die Akteure sind nicht allein die Bediener oder „Verlängerungen" der Technik oder, andersherum gesehen, die Systeme nicht mehr die Verbesserung des „Mängelwesens Mensch", der möglicherweise gar als Störfaktor betrachtet wird. Es sind nicht allein die Normen- und Gesetzgeber, die den Umgang mit Gefahren im Bereich der Techniknutzung und Technikdokumentation regeln, sondern auch die Nutzer und Dritte (Betroffene) melden Interesse und Bedarf nach Information und Partizipation an. So stellen sich Fragen nach der Beteiligung der Nutzer an der Technikentwicklung im Bereich der Techniksicherheit.

8 Die Thematik „Risiko/Sicherheit" ist in zwei Forschungsprojekten bearbeitet worden: (i) NORMA (BMBF-Projekt: NutzerOrientiertes RisikoMAnagement, 2001-2003, Hannover; (ii) MULTH (EU-Projekt, Multilingualer Thesaurus und Hypertext, mit Industriepartnern und den Universitäten Strasbourg, Wien, Duisburg-Essen, Chemnitz, 2005-2008).

9 Rothkegel 2009; Rothkegel/Villiger 2005.







„Information in der und für die Kommunikation" bedeutet, dass neben dem Sachbezug der Personenbezug mit allen Konsequenzen in den Blick kommt, was über ein einfaches Transportmodell der Kommunikation mit Sender und Empfänger hinausgeht. In den Blick kommt dabei, dass wir es nicht mit dem Transport von Information von einem Sender zum Empfänger (Containermodell der Kommunikation) zu tun haben, sondern mit Wissenstransformationen, die gelingen oder misslingen. Es geht darum, dass wir nicht nur die erwünschte gelingende Kommunikation betrachten, sondern dass wir Fehlkommunikation, Falschverstehen und Nichtverstehen als „Normalfall" einbeziehen. Konflikte kommen zum Tragen nicht nur hinsichtlich der Inhalte, sondern auch im Hinblick auf die Kommunikationsstrategien und deren Ausführungen durch sprachliche und visuelle Mittel. Als Instrumente der Kommunikation sind sie von Inhalten und kommunikativen Funktionen nicht zu trennen und sind auf diese Weise mit beteiligt am Gelingen oder Misslingen. In dieser Sichtweise stellt sich die Frage nach den Sicherheitsmodellen, die unterschiedlichen Kommunikationssituationen zugrunde liegen. Die Kommunikation in und mit der Öffentlichkeit sowie zwischen Experten und Nichtexperten verlangt Betrachtungsweisen, die Wissen als flexible und kontextuelle Größe handhaben. Auch die Medien (Presse, Fernsehen, Internet) als Kommunikationsformen mit eigenen Bedingungen der Informationsbildung und -distribution erfordern Aufmerksamkeit, wenn man die kommunikative Vermittlung von „Sicherheit" verstehen möchte.





1.3 VON DER ERFASSUNG DER SICHERHEIT ZUM RISIKO- UND SICHERHEITS-MANAGEMENT

Die meisten Sicherheits- und Risikoanalytiker sind sich dahingehend einig, dass es wenig Sinn macht, Risiken pauschal zu bewerten.[10] Vor allem auf dem Hintergrund divergierender Präferenzen und Ungleichgewichte bei der Verteilung von Risiken und Chancen müssen *Risiken als heterogene und komplexe Phänomene* angesehen werden, die eine einheitliche Bewertung und Behandlung verbieten. Gleichzeitig ist aber die Risikopolitik überfordert, wenn sie bei jeder riskanten Aktivität eine eigene Strategie zur Beurteilung von Risiken entwickeln und einsetzen würde. Ähnlich wie es bereits heute bei der Bewertung von toxikologischen Risiken üblich ist, ist eine Aufteilung der verschiedenen Risiken in *Risikotypen* oder Risikoklassen notwendig und sinnvoll.[11] Die Einteilung in diese Risikotypen ist vor allem von dem Grundanliegen getragen, typenspezifische Verfahrensweisen und Managementregeln zu entwickeln, die einen den Risiken angemessenen und dem Begrenzungsauftrag angepassten Umgang mit Risiken erlauben.

10 Renn/Walker 2007; National Research Council 1983; Hohenemser et al. 1983; Shrader-Frechette 1991; WBGU 1999.

11 IRGC 2005; Renn/Klinke 2001.





Wegen der Komplexität der Einflussfaktoren auf Risiko und Sicherheit muss aber sowohl bei der Analyse der Risiken als auch bei deren Management ein integrativer und interdisziplinärer Ansatz gewählt werden. Rückblickend auf die (technische) Sicherheitsforschung kann festgestellt werden, dass sich mit der Ausweitung des Forschungsfeldes (komplexere Erfassung von Zusammenhängen und Wechselwirkungen, Einbeziehung von Mensch-Technik-Interaktionen, Verständnis von Technik als sozio-technisches und kulturelles „Phänomen") zugleich der Bereich der involvierten wissenschaftlichen Disziplinen über die Technik- und die Wirtschaftswissenschaften (sowie der mit ihnen verbundenen Naturwissenschaften und Mathematik) hinaus ständig erweitert hat und gegenwärtig auch viele sozial-, kultur- und geisteswissenschaftliche Disziplinen betrifft. Inzwischen ist in der Forschung wie in der Praxis die Notwendigkeit der Synthese von Natur-, Technik- und Verhaltenswissenschaften bei der Klärung von Sicherheitsfragen nicht mehr umstritten. Aber auch die klassischen Geisteswissenschaften wie Philosophie, Technikgeschichte und Sprachwissenschaften können wichtige Beiträge für interdisziplinäre Sicherheits- und Risikoforschung liefern. So beschäftigt sich etwa die Technikphilosophie mit der Klärung grundlegender Begrifflichkeiten (etwa Facetten des Sicherheitsverständnisses), Argumentationen und Begründungsverfahren sowie dem Herausarbeiten impliziter Bedeutungsgehalte und Prämissen. Damit schließt sie sowohl an die Linguistik als auch an die Kulturwissenschaften an. Darüber hinaus formuliert sie spezifische Standards und identifiziert mögliche Kriterien, die bei der Beurteilung von (Technik-) Sicherheit und dem praktischen Umgang mit technisch bedingten Gefährdungen zugrunde zu legen sind (bzw. zugrunde gelegt werden sollten). Der normative Aspekt technischer Sicherheit zeigt sich darin, dass das, was als wünschenswerte bzw. nicht wünschenswerte Folgen technischen Handelns bewertet, was als adäquate bzw. nicht adäquate gesellschaftliche Antwort auf technisch bedingte Problemsituationen betrachtet und welcher Bereich möglicher Gefährdungen wahrgenommen bzw. ausgeblendet wird, von Wert- und Normvorstellungen abhängt – die immer auch kulturell geprägt sind.





Die Einbeziehung der Geistes- und Sozialwissenschaften in die Analyse und für das Management von Risiken verspricht einen Zugewinn an (Technik-) Sicherheit bzw. – andersherum – eine Reduzierung von Risiken. Dabei gewinnen die meisten Risiken, vor allem aber die durch menschliche Aktivitäten ausgelösten Risiken ihre besondere Brisanz nicht oder nicht allein aus den direkten physischen Schäden, sondern aus den weitreichenden, auch transsektoralen Wirkungen, die sie in zentralen gesellschaftlichen Systemen, etwa der Wirtschaft, der Finanzwelt oder dem politischen Institutionensystem,





hervorrufen.[12] Die gesellschaftliche Dynamik von Risikodebatten, von Konfliktöffnung wie -schließung wird daher nicht allein durch physisch-materielle Schadensprozesse bestimmt, sondern wesentlich auch durch Weltbilder, Wertideen, Interessenvertretung und Machtverhältnisse beeinflusst.[13] Die OECD hat diesen Typus des kontext-übergreifenden Risikos mit dem Begriff des systemischen Risikos belegt.[14]

1.4 SYSTEMISCHE RISIKEN ALS BESONDERE GEFÄHRDUNG VON SICHERHEIT

Das Konzept der „systemischen Risiken" geht zunächst einmal von einem realen Beobachtungsgegenstand aus: Auf der einen Seite verringert sich das individuelle Risiko weltweit (mit Ausnahme vieler Transformationsgesellschaften im ehemaligen Ostblock), durch einen technischen Unfall oder durch technisch bzw. zivilisatorisch induzierte Aktivitäten an Leben oder Gesundheit geschädigt zu werden; auf der anderen Seite erhöht sich das kumulierte Katastrophenpotenzial der Wirkungen und deren räumliche und zeitliche Reichweite.[15] Der Grund hierfür liegt in zentralen Modernisierungsprozessen. Dazu gehören die zunehmende Verdichtung menschlicher Siedlungsräume, die Zentralisierung von technischen Produktionsanlagen, die zunehmende Eingriffstiefe in die Natur durch menschliche Aktivitäten sowie die sich beschleunigende globale Vernetzung, die zum Beispiel über den internationalen Warenverkehr transnationale Lebensmittelkrisen hervorbringen kann.




Dieser realen Entwicklung kommt aber in einem zweiten Schritt zentrale symbolische und konstruktive Bedeutung zu: Dabei werden zunächst technische Risiken mit symbolischen Konnotationen versehen, die großen Einfluss auf die intuitive Wahrnehmung und Bewertung ausüben.[16] Darüber hinaus werden riskante Aktivitäten mit bestimmten Interessen, Werten und Weltbildern in Verbindung gebracht, die nur in lockerer Kopplung mit dem physischen Schadenspotenzial stehen, dafür aber eine enge gesellschaftspolitische Verknüpfung mit aktuellen politischen Auseinandersetzungen erlauben.[17] Schließlich ranken sich kulturelle Sinnmuster um riskante Aktivitäten, die von rein symbolischen Verletzungen (etwa von religiösen Gefühlen) bis zu Kombinationen

[12] Auch das Konzept der „gesellschaftlichen Verstärkung von Risiken" („social amplification of risk") hat wichtige theoretische und empirische Hinweise auf solche indirekten, sekundären Risikoeffekte geliefert (Kasperson et al. 1988, Renn et al. 1992). Dieser Analyserahmen fokussiert auf die Auswirkungen, die physische Risiken auf der sozialen und institutionellen Ebene haben. Das Konzept der systemischen Risiken reicht allerdings über die Verstärkung oder Abschwächung von physischen Effekten hinaus. Es zielt auf die Mechanismen, nach denen die verschiedenen Schadenskategorien miteinander interagieren und sich gegenseitig aufschaukeln.

[13] Renn/Keil 2008; Gill 2001.

[14] OECD 2002.

[15] Streffer et al. 2000, S. 311 ff.

[16] Slovic 1992; Jungermann/Slovic 1993; Boholm 1998; Jaeger et al. 2001, S. 101 ff.

[17] Freudenburg/Pastor 1992; Luhmann 1993, S. 155 ff.





von Schaden und Schadenssituation führen.[18] Diese drei konstruktiven Elemente der Risikoverarbeitung durch das Publikum werden in der Regel durch die Medienberichterstattung sozial verstärkt.[19]

Für die zuständigen Institutionen des Risikomanagements ergeben sich dadurch Risiken zweiter Ordnung: Unabhängig von den tatsächlichen oder von ihnen wahrgenommenen Gefährdungen sind sie für sie häufig unberechenbaren sozialen Risiken in Form von politischem Vertrauensverlust, Legitimationsentzug oder Stigmatisierungseffekten ausgesetzt.[20] Ein gestiegenes Gesundheits-, Umwelt- und Sicherheitsbewusstsein begründet zudem als neue kulturelle Orientierung wachsende Ansprüche auf intakte Lebensumstände – etwa ungefährliche Lebensmittel, eine saubere Umwelt und stabile Märkte –, die zunehmend als politisch steuerbar betrachtet werden. Viele Gefährdungen werden als entscheidungsabhängig definiert und sind damit legitimationspflichtig.[21] Vor allem der regelmäßige Rückgriff auf organisierten Technikprotest durch Umweltorganisationen deutet darauf hin, dass Gefahren kaum noch als unvermeidlich betrachtet werden (auch die sogenannten „natürlichen" Gefahren nicht; man denke nur an die jüngsten Flutkatastrophen, die in einen Zusammenhang mit dem anthropogen verursachten Klimawandel gestellt werden). Vor diesem Hintergrund besitzt die Frage nach objektiv steigenden Gefährdungspotenzialen nur bedingte Relevanz, denn Risikokonflikte nehmen auch unabhängig davon zu, ob die Gefahren real wachsen. Die hierdurch aufbrechenden Legitimationsprobleme setzen die verantwortlichen Institutionen von außen und innen unter Handlungsdruck. Entsprechend verstärken sich die Debatten über effektive und legitime Maßnahmen der Risikosteuerung in Wissenschaft, Wirtschaft und Politik.




Der eingespielte Prozess von Risikoabschätzung (wissenschaftliche Charakterisierung des Risikos nach Gefährdungspotenzial, Exposition und Dosiswirkung) und Risikomanagement (Feststellung eines politischen Handlungsdrucks sowie Wahl der geeigneten Instrumente zur Risikominderung) behandelt traditionell die direkten physischen Folgen für Mensch und Umwelt in den jeweiligen staatlichen Grenzen. Im Rahmen des acatech Themennetzwerks Sicherheit muss es deshalb darum gehen, ein interdisziplinäres

18 Douglas/Wildavsky 1982; Rayner 1990; Pidgeon 1992; Jaeger et al. 2001, S. 183 ff.
19 Kasperson et al. 1988; Kasperson 1992.
20 Renn/Keil 2008; Luhmann 1990; Sjöberg 2001.
21 Darin gründet die semantische Unterscheidung zwischen „Gefahr" als externe Bedrohung und „Risiko" als internalisierte Steuerungsaufgabe von Schadensabwehr bei Luhmann 1991.





Forschungsprogramm zu entwickeln, das die technischen, naturwissenschaftlichen, sozialwissenschaftlichen und geisteswissenschaftlichen Elemente der Risikoerfassung wie des Risikomanagements integriert und damit zu einer konzeptionell innovativen und gleichzeitig praxisgerechten Interpretation der Risiken in der reflexiven Modernisierung kommt. Es gilt zu untersuchen, inwieweit sich neue Konzepte entwickeln lassen, die sich gezielt über die primären physischen Schadenswirkungen hinaus auch der sekundären und tertiären Schadenswirkungen technisch-ökologischer Risiken annehmen. Damit soll das Forschungsprogramm zum Thema Sicherheit *einen wichtigen Beitrag zu der Diskussion über die Gestaltungsoptionen und -beschränkungen komplexer Risiken auf theoretischer wie praktischer Ebene leisten. Denn nur so kann das Potenzial von technischen Innovationen optimal genutzt und weiterentwickelt werden.*

1.5 BRENNPUNKT: SICHERHEITSKULTUR



Technikerzeugung wie -nutzung erfolgt in einer (auch) kulturell verfassten „Umwelt", die auch für die Gewährleistung bzw. Realisierung von (Technik-) Sicherheit relevant ist. Ein konzeptioneller Ansatz in dieser Richtung ist der der „Sicherheitskultur". Dieses Konzept ist noch nicht sehr alt und bislang wenig operationalisiert. International wurde es von der International Nuclear Safety Advisory Group (INSAG) im Jahre 1986 als Reaktion auf das Reaktorunglück in Tschernobyl in die Diskussion eingebracht. Mit dem sogenannten Safety-Culture-Konzept hat sie darauf aufmerksam gemacht, dass neben den technischen Maßnahmen auch die soziokulturellen Aspekte von entscheidender Bedeutung sind. Im Jahre 1991 wurde durch eine internationale Beratergruppe der Begriff „Sicherheitskultur" wie folgt definiert und in die Praxis eingeführt: „assembly of characteristics and attitudes in organisations and of individuals which establishes that, as an overriding priority, [nuclear] safety issues receive the attention warranted by their significance".[22] Erfasst, benannt und beschrieben werden somit *auch* kulturbedingte Verhaltensmerkmale, die für die Gewährleistung der Sicherheit technischer Handlungsvollzüge bedeutsam sind. In Bezug auf Techniksicherheit wurden Sicherheitskulturen bisher vor allem in sogenannten Hochrisiko-Technologiebereichen (Kernkraftwerke, Chemieunternehmen, Luftfahrt) als konzeptioneller Ansatz relevant, aber auch im Bereich der IT-Branche oder der Logistik. Zunehmend finden sich Überlegungen zum integrierten betrieblichen Sicherheitsmanagement außerhalb dieses Bereiches. „Sicherheitskul-

[22] Swiss Re 1998, S. 18.







tur" wurde damit zum Schlüsselbegriff für das Sicherheitsverhalten aller Mitarbeiter in einem Unternehmen und in diesem Sinne Teil der Unternehmenskultur. Dabei wird „Sicherheitskultur" nicht nur intra-, sondern – vor allem als Folge von Globalisierungsprozessen – auch interkulturell verstanden.

Deutlich wird, dass „Sicherheitskultur" sowohl eine mehr „theoretische" Ebene (vor allem in Form von Anweisungen, Regeln, Vorschriften, Statements, Codes usw.) als auch eine „praktische" Ebene (als gelebte und praktizierte Sicherheitskultur) besitzt. Oder anders ausgedrückt: Auf der praktischen Ebene umfasst „Sicherheitskultur" die sicherheitsbezogenen Einstellungen, Werte und grundlegenden Überzeugungen der Mitarbeiter bzw. Nutzer. Obwohl seit der „Geburt" des Konzepts der Sicherheitskultur Überlegungen in unterschiedlichen (wissenschaftsdisziplinären) Richtungen erfolgten, ist es jedoch immer noch eher ein programmatischer Ansatz geblieben. Die Gründe dafür sind vielfältig. Genannt seien lediglich drei.





1. Die vorliegenden Überlegungen haben zumeist entweder einen wirtschaftswissenschaftlichen Hintergrund und werden als Aspekt des Unternehmensmanagements (bzw. des Sicherheitsmanagements) eingeführt oder sie kommen aus dem Bereich der sogenannten Arbeitswissenschaften (wie Ergonomie, Arbeits- und Ingenieurpsychologie) und bleiben den jeweiligen disziplinären Paradigmen bzw. Konzeptualisierungen verhaftet.
2. Häufig erfolgt keine Explizierung der zugrunde gelegten theoretischen Annahmen (insbesondere hinsichtlich des Kultur- und Technikverständnisses, der Auffassung vom Menschen und des Konzepts der Mensch-Technik-Interaktion).
3. Eine Operationalisierung (und damit auch Vergleichbarkeit) von Sicherheitskulturen ist derzeit schlecht durchführbar, da (inter- wie intrakulturelle) Indikatoren bislang kaum entwickelt wurden.

Die Erforschung technischer Sicherheitskulturen und deren Gelingensbedingungen halten wir für einen besonders fruchtbaren Ansatz zur Analyse der sicherheitsrelevanten Praxis in Unternehmen und Behörden sowie zur Ableitung von Empfehlungen für praktische Verbesserungen im Management von Risiken. Auf welche Themen diese Forschung besonders gelenkt werden soll, wird im nachfolgenden Abschnitt beschrieben.





1.6 DRINGENDE FORSCHUNGSFRAGEN UND -BEREICHE

Die acatech Arbeitsgruppe „Sicherheit und Risiko" hat die Aufgabe, Leitlinien für ein Forschungsprogramm auf dem Gebiet „Interdisziplinäre Risikoforschung" zu erarbeiten und dabei die Forschungsaufgaben und Forschungsziele zu identifizieren, die einen hohen Problemdruck und einen steigenden Handlungsbedarf signalisieren. Aus jetziger Sicht bieten sich fünf Forschungsfelder als besonders dringlich an:

- Erstens ist die Frage nach der angemessenen Organisationsform und erfolgversprechenden Instrumenten bei der Vorsorge gegen eine Kombination von technischen Risiken mit Elementarrisiken wie Überflutung, Sturm und Erdbeben zu erwähnen. Das Problem liegt im Wesentlichen darin, dass die Unsicherheit über die Höhe des Schadens wie auch über die Wahrscheinlichkeiten des Eintretens solcher Schäden aufgrund klimatischer Veränderungen und anderer globaler Wandlungsprozesse wächst. Dazu kommt das Problem der Moral Hazards, dass die Geschädigten Ausgleichszahlungen vom Staat erwarten und daher weder an Prävention noch an Vorsorge interessiert sind. Um diese Probleme anzugehen, sind zum einen linguistische und sozialwissenschaftliche Studien zur Wahrnehmung und Bewertung von Kombinationsrisiken vonnöten, zum anderen müssen neue Formen der Versicherung oder Private-Public-Partnershipmodelle entworfen und erprobt werden. In diesem Forschungsfeld ist vor allem die partizipative Vorgehensweise unter Einbeziehung der Regulierer, der Versicherer und der betroffenen Bürger(innen) unerlässlich, um zu praktikablen und akzeptablen Lösungen zu kommen.




- Zweitens stellt sich die Frage nach regional integrierten Risikoanalysen mit Handlungshinweisen für eine Entzerrung von Risikoakkumulationen. Das Problem in diesem Bereich besteht in der regionalen Verdichtung von Anlagen mit einem meist geringen Risikopotenzial pro Anlage, aber mit einem signifikanten Risikopotenzial für die Anlagen in ihrer Gesamtheit. So wachsen oft Siedlungen in die Nähe von Gastanks oder Chemikalienlager, Tankstellen entstehen neben feuergefährdeten Chemieanlagen oder Anlagen mit Gefahrstoffen liegen in den Einflugschneisen von Flughäfen. Jede dieser Einzelanlagen birgt nur ein kleines Risiko, das den Grenzwerten für eine Genehmigung auch genügt, aber die Synergieeffekte zwischen den Anlagen können zu einer erheblichen Erhöhung des Risikos führen. Hier sind neue technische, politische und kommunikative Instrumente zu entwickeln, die eine regional integrierte Risikoabschätzung unter Einbeziehung der jeweils betroffenen Akteure ermöglichen und gleichzeitig Optionen zur Verringerung des aggregierten Risikos entwickeln helfen. Darüber hinaus sind auch ethische und rechtliche Aspekte der Zurechenbarkeit von Verantwortung bei diffusen Risikoeinträgen besonders bedeutsam.





- Drittens ist es wichtig, die Frage nach dem Umgang mit systemischen Risiken mit einem hohen Anteil an sekundären Folgen einzubeziehen. Das Problem besteht hier darin, dass die klassischen Institutionen des Risikomanagements zwar gelernt haben, die physischen Risiken von Technologien und Aktivitäten angemessen zu erfassen und effektiv zu begrenzen, sie jedoch weder das theoretische Rüstzeug noch die praktischen Erfahrungen mitbringen, wie man effektiv und vorsorgeorientiert mit Sekundärfolgen wie finanziellen, ökonomischen, politischen, sozialen und psychischen Auswirkungen umgehen soll. Die Problemlösung in diesen Fällen setzt nicht nur neue interdisziplinäre Perspektiven voraus, sondern auch die Entwicklung von Instrumenten zur Früherkennung von gesellschaftlichen Kontroversen und Konflikten sowie die umsetzungsorientierte Erprobung von neuen Verfahren der Beteiligung von Betroffenen an Planungsprozessen.
- Viertens ist die empirische Erforschung von Governance-Prozessen im Bereich von Risikovorsorge und Sicherheitspolitik relevant. In pluralen Gesellschaften werden Fragen des Risikomanagements nicht mehr allein vom Staat und von Wirtschaftsunternehmen aufgegriffen, sondern auch von vielen Akteuren der Zivilgesellschaft. Die Kooperation zwischen Staat, Wirtschaft, Wissenschaft und Zivilgesellschaft ist oft zielführend für die Verbesserung der Sicherheit, oft aber auch innovationshemmend oder sogar kontraproduktiv. Zudem sind die Managementsysteme innerhalb von Unternehmen und Behörden nicht immer ausreichend, um den entsprechenden Schutz zu bieten. Für die Erfassung von Governance-Strukturen und deren Optimierung sind vor allem politikwissenschaftliche, institutionenökonomische und soziologische Ansätze von besonderer Bedeutung. Diese müssen dann mit den entsprechenden technischen und naturwissenschaftlichen Sicherheitsstudien verknüpft werden, damit physische Wirksamkeit der Risikobegrenzung und institutionelle Angemessenheit des Risikomanagements Hand in Hand gehen können.
- Fünftens ist die Frage nach dem Umgang mit sozialen Risiken wie Terrorismus und Sabotage bis heute weitgehend ungeklärt. Viele technische Anlagen sind sicherheitstechnisch so ausgelegt, dass sie gegen technische Störungen im Betriebsablauf und auch gegen zufällige Fehlbedienungen ein ausreichendes Maß an Sicherheitspuffer bieten. Wird jedoch eine Absicht der Zerstörung bzw. eine vorsätzliche Auslösung des Gefahrenpotenzials unterstellt, versagen diese Sicherheitsbarrieren häufig. Hier sind neue Konzepte gefragt, die zum einen auf technische Resilienz aufbauen und zum anderen auf psychologisch nachvollziehbare Szenarien der Bedrohung zurückgreifen. In diesem Feld sind auch geisteswissenschaftliche Perspektiven, von der Geschichtsforschung bis zur Kulturforschung des Terrorismus, von besonderem Wert.








1.7 LITERATUR

Banse 1996
Banse, G.: „Herkunft und Anspruch der Risikoforschung." In: Ders. (Hrsg.): Risikoforschung zwischen Disziplinarität und Interdisziplinarität, Berlin: Edition Sigma, 1996, S. 15-72.

Beck 1986
Beck, U.: Die Risikogesellschaft. Auf dem Weg in eine andere Moderne, Frankfurt/Main: Suhrkamp, 1986.

Boholm 1998
Boholm, A: "Comparative Studies of Risk Perception: A Review of Twenty Years of Research." Journal of Risk Research 1 (1998), Nr. 2, S. 135-163.

Douglas 1966
Douglas M.: Purity and Danger: Concepts of Pollution of Taboo, London: Routledge and Kegan Paul, 1966.

Douglas/Wildavsky 1982
Douglas, M./Wildavsky, A.: Risk and Culture, Berkeley: University of California Press, 1982.

Ewald 1993
Ewald, F.: Der Vorsorgestaat, Frankfurt/Main: Suhrkamp, 1993.

Freudenburg/Pastor 1992
Freudenburg, W. R./Pastor, S. K.: "Public Responses to Technological Risk: Toward a Sociological Perspective." In: Sociological Quarterly 33 (1992), Nr. 3, S. 389-412.

Gill 2001
Gill, B.: Kosmologisches Denken. Über die Wirkung von Naturvorstellungen in Technik- und Umweltkonflikten, (Habilitationsschrift, Ludwig-Maximilians-Universität), München, 2001.

Hohenemser et al. 1983
Hohenemser, C./Kates, R. W./Slovic, P.: "The Nature of Technological Hazard." In: Science 220 (1983), S. 378-384.





IRGC 2005
International Risk Governance Council (IRGC): Risk Governance: Towards an Integrative Approach, (White Paper No. 1, written by O. Renn with an annex by P. Graham), Genf: IRGC, 2005.

Jaeger et al. 2001
Jaeger, C./Renn, O./Rosa, E./Webler, T.: Risk, Uncertainty and Rational Action, London: Earthscan, 2001.

Jungermann/Slovic 1993
Jungermann, H./Slovic, P.: „Charakteristika individueller Risikowahrnehmung." In: Krohn, W./Krücken, G. (Hrsg.): Riskante Technologien: Reflexion und Regulation. Frankfurt/Main: Suhrkamp, 1993, S. 79-100.

Kasperson 1992
Kasperson, R. E.: "The Social Amplification of Risk: Progress in Developing an Integrative Framework." In: Krimsky, S./Golding, D. (Hrsg.): Social Theories of Risk, Westport: Praeger, 1992.



Kasperson et al. 1988
Kasperson, R. E./Renn, O./Slovic, P./Brown, H. S./Emel, J./Goble, R./Kasperson, J. S./Ratick, S.: "The Social Amplification of Risk: A Conceptual Framework." In: Risk Analysis 8 (1988), S. 177-187.

Luhmann 1990
Luhmann, N.: "Technology, Environment, and Social Risk: A Systems Perspective." In: Industrial Crisis Quarterly 4 (1990), S. 223-231.

Luhmann 1991
Luhmann, N.: Soziologie des Risikos, Berlin: Springer, 1991.

Luhmann 1993
Luhmann, N.: „Risiko und Gefahr." In: Krohn, W./Krücken, G. (Hrsg.): Riskante Technologien: Reflexion und Regulation, Frankfurt/Main: Suhrkamp, 1993, S. 138-185.

Markowitz 1990
Markowitz, J.: „Kommunikation über Risiken – Eine Theorie-Skizze." In: Schweizerische Zeitschrift für Soziologie 3 (1990), S. 385-420.





NRC 1983
National Research Council, Committee on the Institutional Means for Assessment of Risks to Public Health (NRC): Risk Assessment in the Federal Government: Managing the Process, Washington: National Academy Press, 1983.

OECD 2003
OECD: Emerging Systemic Risks. Final Report to the OECD Futures Project, Paris: OECD Press, 2003.

Pidgeon 1997
Pidgeon, N. F.: "The Limits to Safety? Calture, Politics, Learning and Manmade Disasters." In: Journal of Contingencies and Crisis Management 5 (1997), Nr. 1, S. 1-14.

Rayner 1990
Rayner, S.: Risk in Cultural Perspective: Acting under Uncertainty, Dordrecht, Boston: Kluwer, 1997.

Renn 2008
Renn, O.: Risk Governance. Coping with Uncertainty in a Complex World, London: Earthscan, 2008.



Renn/Keil 2008
Renn, O./Keil, F.: „Systemische Risiken: Versuch einer Charakterisierung." In: GAIA – Ökologische Perspektiven für Wirtschaft und Gesellschaft 4 (2008), Nr. 17, S. 349-354.

Renn/Klinke 2001
Renn, O./Klinke, A.: "Environmental Risk – Perception, Evaluation and Management: Epilogue." In: Böhm, G./Nerb, J./McDaniels, T./Spada, H. (Hrsg.): Environmental Risks: Perception, Evaluation and Management, Amsterdam: Elsevier Science, 2001, S. 275-299.

Renn/Walker 2007
Renn, O./Walker, K.: "Lessons Learned. A Re-Assessment of the IRGC Framework on Risk Governance." In: Renn, O./Walker, K. (Hrsg.): Global Risk Governance. Concept and Practice Using the IRGC Framework, (International Risk Governance Council Bookseries 1), Berlin, Heidelberg: Springer, 2007, S. 331-360.





Renn et al. 1992
Renn, O./Burns, W. J./Kasperson, J. X./Kasperson, R. E./Slovic, P.: "The Social Amplification of Risk: Theoretical Foundations and Empirical Applications." In: Journal of Social Issues 48 (1992), Nr. 4, S. 137-160.

Renn et al. 2007
Renn, O./Schweizer, P.-J./Dreyer, M./Klinke, A.: Risiko. Über den gesellschaftlichen Umgang mit Unsicherheit, München: ÖKOM Verlag 2007.

Rothkegel 2000
Rothkegel, A.: "Transfer of Knowledge in Cross-Cultural Discourse." In: Jarvella, R./ Lundquist, L. (Hrsg.): Language, Text, and Knowledge. Berlin: Mouton, de Gruyter, 2000, S. 189-206.

Rothkegel 2008
Rothkegel, A.: „Wissenssysteme und ihre konzeptuellen Transformationen in der Experten/Nichtexperten-Kommunikation: Technikkommunikation in kultureller Perspektive." In: Rösch, O. (Hrsg.): Technik und Kultur. Berlin: Verlag News & Media, 2008, S. 48-60.



Rothkegel 2009
Rothkegel, A.: Technikkommunikation. Linguistische Grundlagen der Medien-Wissens- und Textarbeit, Wien, Konstanz: UTB 2009 (im Erscheinen).

Rothkegel/Villiger 2005
Rothkegel, A./Villiger, C.: „Modellierung von Risikowissen und multilinguale Textproduktion." In: Braun, S./Kohn, K. (Hrsg.): Sprache(n) in der Wissensgesellschaft, Frankfurt: Lang, 2005, S. 205-212.

Shrader-Frechette 1991
Shrader-Frechette, K. S.: Risk and Rationality. Philosophical Foundations for Populist Reforms, Berkeley: University of California Press, 1991.

Slovic 1992
Slovic, P.: "Perceptions of Risk: Reflections on the Psychometric Paradigm." In: Krimsky, S./Golding, D. (Hrsg.): Social Theories of Risk, Westport: Praeger, 1992, S. 153-178.





Sjöberg 2001
Sjöberg, L.: "Political Decisions and Public Risk Perception." In: Reliability Engineering & System Safety 72 (2001), S. 115-123.

Streffer et al. 2000
Streffer, C./Bücker, J./Cansier, A./Cansier, D./Gethmann, C. F./Guderian, R./Hanekamp, G./ Henschler, D./Pöch, G./Rehbinder, E./Renn, O./Slesina, M./Wuttke, K.: Umweltstandards. Kombinierte Expositionen und ihre Auswirkungen auf den Menschen und seine Umwelt, Berlin: Springer, 2000.

Swiss Re 1998
Swiss Re: Safety Culture – a Reflection of Risk Awareness, Zürich: Swiss Reinsurance Company, 1998.

Wiedemann 1993
Wiedemann, P. M.: „Tabu, Sünde, Risiko: Veränderungen der gesellschaftlichen Wahrnehmung von Gefährdungen." In: Bayerische Rückversicherung (Hrsg.): Risiko ist ein Konstrukt. Wahrnehmungen zur Risikowahrnehmung, München: Knesebeck, 1993, S. 43-67.




Wildavsky 1984
Wildavsky, A.: „Die Suche nach einer fehlerlosen Risikominderungsstrategie." In: Lange, S. (Hrsg.): Ermittlung und Bewertung industrieller Risiken, Berlin: Springer, 1984, S. 224-233.

WBGU 1999
Wissenschaftlicher Beirat der Bundesregierung Globale Umweltveränderungen (WBGU): Welt im Wandel: Der Umgang mit globalen Umweltrisiken, Berlin: Springer 1999.



2 SICHERHEIT, RISIKO UND VERTRAUEN

ORTWIN RENN

2.1 EINLEITUNG

Um das komplexe Verhältnis von Sicherheit, Risikoempfinden und Vertrauen in Institutionen der Risikoregulierung und des Risikomanagements näher zu beleuchten, ist eine Einführung in die Grundmechanismen der Risikowahrnehmung sinnvoll. Auf dieser Basis können auch die Rolle des Vertrauens besser abgeschätzt und offene Forschungsfragen artikuliert werden. Deshalb werden in den folgenden Abschnitten die grundlegenden Erkenntnisse der Wahrnehmungsforschung rekapituliert und auf ihre Bedeutung für die Frage nach dem Vertrauen analysiert.

2.2 GRUNDLAGEN DER RISIKOWAHRNEHMUNG

Unter dem Begriff der Wahrnehmung werden in der kognitiven Psychologie alle mentalen Prozesse verstanden, mit denen eine Person über die Sinne Signale aus der physischen Umwelt ebenso wie Informationen durch Kommunikation aufnimmt, verarbeitet und auswertet.[1] Wahrnehmungen sind eine Realität eigener Natur: So wie in Zeichentrickfilmen die gemalten Figuren erst dann in den Abgrund stürzen, wenn sie mitten in der Luft stehend plötzlich der Gefahr gewahr werden, so konstruieren auch Menschen ihre eigene Realität und stufen Risiken nach ihrer subjektiven Wahrnehmung ein. Diese Form der intuitiven Risikowahrnehmung basiert auf der Vermittlung von Informationen über die Gefahrenquelle, den psychischen Verarbeitungsmechanismen von Unsicherheit und früheren Erfahrungen mit Gefahren. In diese Wahrnehmungen fließen eigene Interessen, Werthaltungen, Interpretationen der Wirklichkeit, Vertrauen in Experten und Regulationsbehörden und anderes mehr ein.[2] Die subjektbezogene Risikowahrnehmung ist nicht an stringenten Kriterien der methodisch orientierten Risikoabschätzung ausgerichtet, sondern beruht auf subjektiven Erfahrungen, eigenen Erlebnissen und Sinneseindrücken sowie vermittelten Informationen und interessengeleiteten Einschätzungen. Diese folgen aber quasi-universellen, übergesellschaftlichen Heurismen der Urteilsbildung, die sich im Prozess der Sozialisierung und Enkulturation bei Individuen und Gruppen innerhalb eines Kulturkreises oder einer Bezugsgruppe herausgebildet haben.[3]

---

1 Jungermann/Slovic 1993b.
2 Slovic 1987; Fischhoff 1995; Rohrmann/Renn 2000.
3 Renn/Rohrmann 2000.





Wahrnehmungsmuster sind relativ gut in der Psychologie und Sozialpsychologie untersucht. Es ist nicht so, dass Menschen völlig beliebig zusammengefügte Strategien zur Bewertung von Informationen benutzen, sondern sie folgen meist relativ konsistenten Mustern der Urteilsbildung. Diese Muster beziehen sich auf evolutiv gewachsene Grundlagen der Gefahrenabwehr.[4] In Gefahrensituationen reagiert der Mensch mit vier genuinen Strategien: *Flucht, Kampf, Totstellen und gegebenenfalls neugieriges Experimentieren (auf der Basis von Versuch und Irrtum)*. Man kann sich dieses Reaktionsmuster vergegenwärtigen, wenn man sich vorstellt, wie unsere Vorfahren in der Wildnis einem Raubtier begegnet sind. In dieser Situation einer akuten Bedrohung, etwa einer Begegnung mit einem Tiger, haben die Menschen nur drei Möglichkeiten: erstens zu fliehen, in der Hoffnung, schneller zu sein als der Tiger, zweitens auf die eigene Stärke zu bauen, um es mit dem Tiger aufnehmen zu können, oder drittens sich tot zu stellen in der Hoffnung, man könne den Tiger täuschen. Die letzte Möglichkeit des Experimentierens hat in diesem Fall nur der Tiger.

Diese Grundmuster der Wahrnehmung haben sich in der Evolution der menschlichen Kulturen zunehmend mit kulturellen und sozialen Mustern angereichert. Die kulturellen Muster lassen sich durch sogenannte qualitative Risikomerkmale beschreiben. Sie orientieren sich an bestimmten Eigenschaften von Risiken oder riskanten Situationen, und zwar zusätzlich zu den beiden klassischen Faktoren der Risikoabschätzung, der Höhe der Wahrscheinlichkeit und der Höhe des möglichen Schadens. Dabei unterscheiden die Wahrnehmungsforscher zwei Klassen von qualitativen Wahrnehmungsmustern.[5] Zum einen sind dies die *risikobezogenen Muster*, die auf Eigenschaften der Risikoquelle bezogen sind. Darunter fallen:

- Gewöhnung an die Risikoquelle,
- Katastrophenpotenzial der Risikoquelle,
- Sicherheit fataler Folgen bei Gefahreneintritt,
- unerwünschte Folgen für kommende Generationen,
- sinnliche Wahrnehmbarkeit von Gefahren und
- Eindruck der Reversibilität der Risikofolgen.

Ein Beispiel dieser risikobezogenen Muster ist die wahrgenommene „Schrecklichkeit" der Folgen eines Schadeneintritts. Dies lässt sich anhand eines Vergleichs der subjektiven Einschätzung der Risiken des Autofahrens und des Fliegens mit einem Passagierflugzeug illustrieren. Statistisch gesehen ist die Wahrscheinlichkeit, bei einem Autounfall zu Schaden zu kommen, viel höher als die Wahrscheinlichkeit eines Flugzeugabsturzes. Der entscheidende Unterschied zwischen beiden Beförderungsweisen liegt in der wahr-

4 Renn 2005.
5 Fischhoff et al. 1978; Covello 1983; Jungermann/Slovic 1993a; Boholm 1998; Renn 2004.





genommenen Schrecklichkeit des Schadensfalls. Da beim Fliegen zumeist katastrophale Folgen für die Mehrzahl der Reisenden zu erwarten sind, beim Autofahren jedoch nur Einzelne betroffen sind, die zudem damit rechnen, mit einem Blechschaden das Unglück zu überstehen, liegt die wahrgenommene Schrecklichkeit der Risiken des Fliegens deutlich höher als jene des Autofahrens. Das Gefühl der Ausweglosigkeit beim Fliegen ist furchteinflößend, weil es die typischen Reaktionsmuster von Flucht, Kampf oder Totstellen nicht mehr als sinnvolle Strategien der Gefahrenabwehr zulässt.

Zum anderen werden *situationsbezogene Muster* unterschieden, die auf die Eigenarten der riskanten Situation ausgerichtet sind.[6] Darunter fallen:

- persönliche Kontrollmöglichkeit des Risikoanteilsgrades,
- Freiwilligkeit der Risikoübernahme,
- Eindruck einer gerechten Verteilung von Nutzen und Risiko,
- Kongruenz zwischen Nutznießer und Risikoträger,
- Vertrauen in die öffentliche Kontrolle und Beherrschung von Risiken,
- Erfahrungen (kollektiv wie individuell) mit Technik und Natur,
- Vertrauenswürdigkeit der Informationsquellen und
- Eindeutigkeit der Informationen über Gefahren.

Ein Beispiel für situationsbezogene Muster der Wahrnehmung ist die persönliche Kontrollfähigkeit. Wenn jemand der Meinung ist, er könne das Risiko selbst steuern, dann empfindet er dies als weniger gravierend. Bei Essgewohnheiten kommt dieser Heurismus oft zum Tragen. Menschen glauben, auf Süßigkeiten, Alkohol oder andere als ungesund eingestufte Lebensmittel leicht verzichten zu können, wenn sie es nur wollten. Dagegen werden meist harmlose chemische Zusatzstoffe in Lebensmitteln als ernsthafte Bedrohung der eigenen Gesundheit erlebt.[7]

Ein für den Zweck dieses Beitrags besonders relevantes Muster betrifft das Vertrauen in die Informationsquellen.[8] Gerade bei solchen Risiken, deren potenzielle Gefahr nicht durch unsere Sinne wahrnehmbar ist, muss sich die betroffene Person auf die Vertrauenswürdigkeit der Institutionen, die eine Risikoabschätzung und darauf aufbauend das Risikomanagement durchführen, verlassen können. Ist dieses Vertrauensverhältnis gestört, kommt es zu Konflikten und häufig zur Forderung von Nullrisiko, weil den Regulierungsversuchen der zuständigen Risikomanager eine objektive Abwägung nicht zugetraut wird (siehe dazu später mehr).

Die Bedeutung der qualitativen Merkmale zur Beurteilung von Risiken bietet eine nahe liegende Erklärung für die Tatsache, dass ausgerechnet diejenigen Risikoquellen, die bei der technisch-wissenschaftlichen Risikoabschätzung als besonders risikoarm ab-

6 Slovic/Fischhoff 1982; Slovic 1987 und 1992; Rohrmann/Renn 2000.
7 De Jonge et al. 2007.
8 Slovic 1993; Blackburn 1998; Cvetkovich 1999; Siegrist/Cvetkovich 2000; Löfstedt 2005.







schneiden, bei der Bevölkerung den größten Widerstand auslösen. Die als kontrovers angesehenen Risikoquellen, wie etwa die Gentechnik oder die Kernenergie, werden besonders häufig mit negativ geladenen Attributen in Verbindung gebracht, Freizeitrisiken dagegen mit eher positiven Attributen assoziiert.

2.3 „MENTALE SCHUBLADEN" DER RISIKOWAHRNEHMUNG

Wenn man diese qualitativen Merkmale gemeinsam betrachtet, so lassen sie sich in einige wenige, in sich schlüssige Risikowahrnehmungsklassen einordnen. Diese werden in der Literatur auch als „semantische Risikomuster" bezeichnet.[9] Besonders gut untersucht sind dabei die folgenden Muster:

Risiko als unmittelbare Bedrohung: Große Störfälle, verbunden mit dem Ausfall von Sicherheitssystemen können bei vielen technischen Systemen, vor allem Großtechnologien, katastrophale Auswirkungen auf Mensch und Umwelt auslösen. Die technische Sicherheitsphilosophie zielt meist auf eine Verringerung der Eintrittswahrscheinlichkeit eines solchen Versagens ab, sodass das Produkt aus Wahrscheinlichkeit und Ausmaß denkbar klein wird. Die stochastische Natur eines solchen Ereignisses macht aber eine Voraussage über den Zeitpunkt des Eintritts unmöglich. Folglich kann das Ereignis in der Theorie zu jedem Zeitpunkt eintreten, wenn auch mit jeweils extrem geringer Wahrscheinlichkeit. Wenn wir uns jedoch im Bereich der Wahrnehmung von seltenen Zufallsereignissen befinden, spielt die Wahrscheinlichkeit eine geringe Rolle: Die Zufälligkeit des Ereignisses ist der eigentliche Risikofaktor. Beispiele für Risikoquellen, die in diese Kategorie fallen, sind große technische Anlagen wie etwa Kernkraftwerke, Flüssiggaslager, chemische Produktionsstätten und andere menschlich geschaffene Gefahrenpotenziale, die im Schadensfall katastrophale Auswirkungen auf Mensch und Umwelt haben können.

Die Vorstellung, das Ereignis könne zu jedem beliebigen Zeitpunkt die betroffene Bevölkerung treffen, erzeugt das Gefühl von Bedrohtheit und Machtlosigkeit. Instinktiv können die meisten Menschen mental (ob real, mag hier dahingestellt bleiben) besser mit Gefahren fertig werden, wenn sie auf sie vorbereitet und eingestellt sind. Ebenso, wie sich die meisten Menschen in der Nacht mehr fürchten als am Tage (obwohl das objektive Risiko, über Tag zu Schaden zu kommen, wesentlich höher ist als während der Nacht, man aber in der Nacht leichter von möglichen Gefahren überrascht werden kann), so fühlen sich die meisten mehr von potenziellen Gefahren bedroht, die sie unerwartet und unvorbereitet treffen, als von Gefahren, die entweder regelmäßig auftreten oder die genügend Zeit zwischen auslösendem Ereignis und möglicher Gefahrenabwehr erlauben. Somit ist das Ausmaß des Risikos in dem hier vorliegenden Verständnis eine Funktion von drei Faktoren: *der Zufälligkeit des Ereignisses, des erwarteten maximalen Schadensausmaßes und der Zeitspanne zur Schadensabwehr.* Die Seltenheit des Ereig-

[9] Renn 1989; Streffer et al. 2003, S. 269 ff.; Renn 2004.







nisses, also der statistische Erwartungswert, ist dagegen unerheblich. Im Gegenteil: häufig auftretende Ereignisse signalisieren eher eine kontinuierliche Folge von Schadensfällen, auf die man sich im „trial and error"-Verfahren einstellen und vorbereiten kann.

Die Wahrnehmung des Risikos als drohende Katastrophe bestimmt häufig die Bewertung technischer Risiken, findet aber nur wenig Anwendung in der Bewertung naturgegebener Katastrophen. Erdbeben, Überflutungen oder Wirbelstürme folgen den gleichen Bestimmungsgrößen wie Großtechnologien, das heißt sie treten relativ selten auf und lassen meist nur wenig Zeit zur Gefahrenabwehr. Jedoch werden sie mit einem anderen, im Folgenden beschriebenen Risikokonzept bewertet.

Risiko als Schicksalsschlag: Natürliche Belastungen und Risiken werden als vorgegebene, quasi unabdingbare Schicksalsschläge betrachtet, während technische Risiken als Konsequenzen von Entscheidungen und Handlungen angesehen werden. Diese Handlungen werden nach anderen Maßstäben bewertet und legitimiert. Im Gegensatz zur Situation der technischen Bedrohung ist die Zufälligkeit des Ereignisses nicht der Angst auslösende Faktor (weil „Zufall" hier Schicksal und nicht die unvorhersehbare Verstrickung von Fehlverhalten beinhaltet). Im Gegenteil ist die relative Seltenheit des Ereignisses ein psychischer Verstärker für die Verneinung der Gefahr.

Durch die zunehmende Beeinflussung natürlicher Katastrophen durch menschliche Aktivitäten ist das Risikomuster des Schicksalsschlags vermehrt mit Merkmalen der Risikowahrnehmung als von Menschen geschaffene Bedrohung durchmischt worden. Dies drückt sich beispielsweise dadurch aus, dass nach Naturkatastrophen immer häufiger die Frage nach der Verantwortung gestellt wird und dabei auch die Unterlassung von möglichen vorbeugenden oder nachsorgenden Maßnahmen als Schuld angesehen wird.[10]

Risiko als Herausforderung der eigenen Kräfte: Eine weitere Bedeutung des Risikobegriffs erschließt sich aus der freiwilligen Übernahme von Risiken als Herausforderung der eigenen Kräfte. Risikoreiches Bergsteigen, zu schnelles Autofahren und Bungee-Springen gehören zum Beispiel in diese Kategorie der „Freizeitrisiken". Bei diesen Freizeitaktivitäten wird nicht, wie vielfach behauptet, das Risiko in Kauf genommen, um einen angenehmen Nutzen zu haben (etwa Wind um die Ohren oder schöne Aussicht), sondern das Risiko ist der Nutzen: Die Aktivitäten gewinnen ihren Reiz gerade dadurch, dass sie mit Risiken verbunden sind.[11]

In all diesen Fällen gehen Menschen Risiken ein, um ihre eigenen Kräfte herauszufordern und den Triumph eines gewonnenen Kampfes gegen Naturkräfte oder andere Risikofaktoren auszukosten. Sich über die Natur oder Mitkonkurrenten hinwegzusetzen und durch eigenes Verhalten selbst geschaffene Gefahrenlagen zu meistern, ist der wesentliche Ansporn zum Mitmachen. Möglicherweise bietet unsere „Absicherungsgesellschaft" zu wenige riskante Herausforderungen, sodass – häufig instinktiv verankerte –

[10] Wiedemann 1993; Jaeger et al. 2001, S. 95 ff.
[11] Machlis/Rosa 1990.







Bedürfnisse nach Abenteuer und Risiko unbefriedigt bleiben. So werden künstliche Situationen geschaffen, die ein kalkulierbares und durch persönlichen Einsatz beherrschbares Risiko bergen, dem man sich freiwillig aussetzt. Risiko als Herausforderung ist an eine Reihe von situationsspezifischen Attributen gebunden, die bereits oben bei der Diskussion um qualitative Faktoren der Risikowahrnehmung angesprochen wurden:

- Freiwilligkeit,
- persönliche Kontrollierbarkeit und Beeinflussbarkeit des Risikos,
- zeitliche Begrenzung der Risikosituation,
- die Fähigkeit, sich auf die riskante Tätigkeit vorzubereiten und entsprechende Fertigkeiten einzuüben, und
- soziale Anerkennung, die mit der Beherrschung des Risikos verbunden ist.

Risiko als Herausforderung ist eine so dominante Handlungsmotivation, dass Gesellschaften symbolische Gefahrensituationen in Form von Sportaktivitäten, Gesellschaftsspielen, Spekulantentum, Geldgeschäften und politischen Spielregeln des Machterwerbs entwickelt haben, um das „Prickeln" bei der Beherrschung von Gefahren zu kanalisieren und die möglichen negativen Konsequenzen durch symbolische Bestrafungen zu ersetzen.[12] Mit der Kanalisierung des Risikorausches geht auch eine symbolische Vorwegnahme realer Gefahren in Form von Computersimulationen und hypothetischen Risikoberechnungen einher.[13] Die herkömmliche Methode, durch Versuch und Irrtum technische Innovationen oder neue Einsatzgebiete für Technik zu überprüfen, ist in einer auf die Erhaltung des Individuums fixierten Gesellschaft moralisch nicht mehr zu rechtfertigen. An die Stelle des – immer Schaden erzeugenden – Irrtums tritt die symbolische Antizipation des Schadens: Abenteuerurlaub darf nur die Illusion der Gefahr vermitteln, aber niemand soll tatsächlich zu Schaden kommen; technische Systeme müssen so angelegt sein, dass sie auch bei Versagen niemanden schädigen können (das Lernen an realen Fehlern wird durch Computersimulation von hypothetischen Schadensabläufen ersetzt); und geplante soziale Veränderungen bedürfen einer wissenschaftlichen Folgenabschätzung inklusive Kompensationsstrategien für potenzielle Geschädigte, bevor eine Reform in Kraft treten kann.



Das zunehmende Erlebnis eines nur symbolischen Schadens schafft natürlich auch neue Erwartungshorizonte gegenüber technischen Systemen. Je mehr der Risikorausch von symbolischen Konsequenzen für einen selbst und mögliche Konkurrenten geprägt ist, desto eher erwartet man auch von den technischen Risikoquellen nur symbolische Konsequenzen. Der echte Schaden darf demnach niemals eintreten.[14]

12 Douglas/Wildavsky 1982.
13 Häfele et al. 1990.
14 Wildavsky 1990.





Risiko als Glücksspiel: Das „Risiko" als Herausforderung, bei der die eigenen Fähigkeiten zur Risikobewältigung den Ausgang der Handlung mitbestimmen, ist nicht identisch mit dem Verständnis von „Risiko" in Lotterien oder Glücksspielen. Verlust oder Gewinn sind hier in der Regel unabhängig von den Fähigkeiten des Spielers. Spielen selbst kann natürlich auch einen Rausch erzeugen und zum Selbstzweck werden, aber es ist die erwartbare oder erhoffte Auszahlung – die Möglichkeit des großen Gewinns –, die das berühmte „Prickeln" erzeugt, und nicht der Vorgang des Spielens (im Gegensatz zu Gesellschaftsspielen, in denen Belohnung und Bestrafung nur noch symbolischen Wert haben).

Psychologen haben sich seit Langem intensiv mit Risikoverhalten bei Glücksspielen befasst. Zum einen lässt sich die Situation im Labor gut simulieren, zum anderen kann man leicht die Abweichungen vom statistischen Erwartungswert bestimmen.[15] Gleich hier soll deutlich werden, dass der statistische Erwartungswert keinen Maßstab für rationales Spielverhalten abgibt. Der Einsatz sollte möglichst gering sein, während der Hauptgewinn ausgesprochen attraktiv sein sollte. Denn Spieler überschätzen die Wahrscheinlichkeit seltener Ereignisse und sind eher bereit mitzuspielen, wenn der Wetteinsatz die Schmerzgrenze nicht überschreitet.

Die Tatsache, dass es jedes Mal einen Gewinner gibt, verführt zu der Vorstellung, man könne selbst der Nächste sein. Häufig werden mit Glücksspielen versteckte Verteilungsideologien (etwa todsichere Wettsysteme, magische Glückszahlen oder ausgleichende Gerechtigkeit) verbunden. So glauben etwa 47 Prozent aller Amerikaner, dass es besondere Glücksnummern gibt, die bestimmten Mitspielern eine bessere Gewinnchance vermitteln.[16] Wird das Zufallsprinzip jedoch anerkannt, dann ist das wahrgenommene Konzept der stochastischen Verteilung von Auszahlungen dem technischen Risikokonzept am nächsten. Nur wird dieses Konzept bei der Wahrnehmung und Bewertung technischer Risiken nicht angewandt. Im Gegenteil: Wie eine Studie in Schweden nachweist, halten es die dort untersuchten Personen geradezu für unmoralisch, eine „Glücksspielmentalität" auf technische Gefahrenquellen, bei denen Gesundheit und Leben auf dem Spiel stehen, anzuwenden.[17]

Risiko als Frühindikator für schleichende Gefahren: Dieses Muster ist für die Frage nach der Rolle des Vertrauens essenziell. Mit der zunehmenden Berichterstattung über Umweltverschmutzung und deren Langzeitwirkungen auf Gesundheit, Leben und Natur haben wissenschaftliche Risikoberechnungen die Funktion von Frühwarnindikatoren erhalten. Nach diesem Risikoverständnis helfen wissenschaftliche Studien schleichende Gefahren frühzeitig zu entdecken und Kausalbeziehungen zwischen Aktivitäten oder Ereignissen und deren latenten Wirkungen aufzudecken. Beispiele für die Verwendung



15 Dawes 1988, S. 92 ff.; Jungermann et al. 2005, S. 181 ff.
16 Miller 1985, Tables 8-13.
17 Sjöberg/Winroth 1985; siehe auch Brehmer 1987.







dieses Risikobegriffs findet man bei der kognitiven Bewältigung von geringen Strahlendosen, BSE, Pestizidrückständen im Trinkwasser, Lebensmittelzusätzen, chemischen Pflanzenschutzmitteln oder genetischen Manipulationen von Pflanzen und Tieren. Gesundheitsrisiken, die aus der Belastung der Umwelt durch menschliche Aktivitäten stammen, werden in der intuitiven Wahrnehmung besonders intensiv empfunden und oft deutlich mehr gefürchtet als vergleichbare Risiken aus dem Lebensalltag, sportlichen Aktivitäten oder aus natürlicher Belastung.[18] Die Wahrnehmung dieser Risiken ist eng mit dem Bedürfnis verknüpft, für scheinbar unerklärliche Folgen (zum Beispiel Robbensterben, Krebserkrankungen von Kindern, Waldsterben etc.) Ursachen ausfindig zu machen. Im Gegensatz zum technisch-medizinischen Risikobegriff wird die Wahrscheinlichkeit eines solchen Ereignisses nicht als eine signifikante (das heißt nicht mehr durch Zufall erklärbare) Abweichung von der natürlich vorgegebenen Variation solcher Ereignisse interpretiert, sondern als Grad der Sicherheit, mit der ein singuläres Ereignis auf eine externe Ursache zurückgeführt werden kann.[19]

Das Wissen um die Möglichkeit von Krebserkrankungen aufgrund einer Umweltbelastung legitimiert zumindest den Verdacht, dass eine Person, die einer bestimmten Umweltbelastung, zum Beispiel den Strahlen einer stationären Mobilfunkantenne, ausgesetzt gewesen ist und die an Krebs erkrankt, aufgrund dieser Belastung erkrankt ist. Wer selbst an Krebs leidet oder mit ansehen muss, wie ein Mitglied der Familie oder des eigenen Freundeskreises von dieser Krankheit getroffen wird, sucht nach einer Erklärung. Metaphysische Erklärungsmuster haben in unserer säkularisierten Welt an Geltung verloren.[20] Gleichzeitig befriedigt das nach heutigem Wissensstand bestmögliche Erklärungsmuster einer zufälligen Verteilung von Krebserkrankungen das psychische Verlangen nach einer „sinnhaften" Erklärung wenig. Es ist trostlos, das zufällige Opfer eines blinden Verteilungsmechanismus von Krankheit zu sein. Kennt man dagegen einen konkreten Grund, etwa Umweltbelastung, Rauchen, falsche Ernährung usw., dann macht das Auftreten der Krankheit zumindest Sinn. Lässt sich aus subjektiver Sicht darüber hinaus eigenes Verschulden (etwa Rauchen oder Alkoholmissbrauch) ausschließen und Fremdverschulden als Ursache der Krankheit heranziehen, dann mag die Krankheit sogar einen sozialen Zweck erfüllen, nämlich die künftigen potenziellen Opfer zu alarmieren und gegen die Ursache des Übels anzukämpfen.




Die häufig hoch emotionale Auseinandersetzung um Risiken dieses Typus muss vor diesem psychischen Hintergrund verstanden werden. Die Befähigung des Menschen zur Empathie verhilft ihm zu einer potenziellen Identifikation mit dem Opfer. Risikoanalysen, die eine bestimmte Wahrscheinlichkeit einer schleichenden Erkrankung aufgrund einer Emission nachweisen, bewirken eine Identifikation mit dem von dem Risiko betroffenen Opfer. Während der Risikoanalytiker stochastische Theorien zur Charakterisierung

[18] Sjöberg 1999a; Rohrmann/Renn 2000.
[19] Kraus et al. 1992.
[20] Wiedemann 1993.





der relativen Gefährdung von Ereignissen benutzt, die keine kausalen Zusammenhänge zwischen singulären Auslösern und deren Effekten erlauben (und damit Distanz zum eigenen Wissensbereich schaffen), sieht der Laie in ihnen den Beweis für die schuldhafte Verstrickung gesellschaftlicher Akteure bei der Verursachung lebensbedrohender Krankheiten.

Bei Risiken als schleichende Gefahren sind die betroffenen Menschen auf Informationen durch Dritte angewiesen. Sie können sie in der Regel nicht sinnlich wahrnehmen. Bewerten sie solche Risiken, dann stoßen sie auf eine Schlüsselfrage: Vertraue ich den Institutionen, die mir dazu die notwendigen Informationen geben? Wenn das Vertrauen nicht gegeben ist, fordern die meisten Menschen Nullrisiko.[21] Denn wenn jemand bei der Bewertung solcher Risiken auf Informationen durch Dritte angewiesen ist, diesen Dritten aber nicht vertraut, dann lässt er sich auf keine Kosten-Nutzen-Bilanz ein. Dann geht er auf „Nummer Sicher", das heißt er ist nicht bereit, ein Risiko für einen bestimmten Nutzen in Kauf zu nehmen. So kann es durchaus psychologisch schlüssig sein, dass jemand die Gesundheitsrisiken gentechnisch veränderter Tomaten als nicht tolerierbar ablehnt, aber gleichzeitig raucht und rasant Auto fährt. Diese Risiken fallen alle in eine andere Wahrnehmungskategorie. Wer den Aussagen der Gentechniker nicht vertraut, wird gentechnisch veränderte Lebensmittel ablehnen, gleichgültig, wie hoch das Risiko für eine Erklärung tatsächlich sein mag.



2.4 STELLENWERT DER RISIKOWAHRNEHMUNG FÜR DEN RATIONALEN UMGANG MIT RISIKEN

Die semantische Bestimmung des Risikobegriffs im Alltagsleben hat zu der wichtigen Erkenntnis geführt, dass der universelle Geltungsanspruch des technischen Risikobegriffs als Maß für die relative Wahrscheinlichkeit von negativen Ereignissen in der Alltagssprache nicht haltbar ist. Begriffe in der Alltagssprache sind gewöhnlich mit mehrfachen Bedeutungen besetzt, die sich für den in der Alltagssprache Kundigen mühelos aus dem Kontext ableiten lassen. Gleichzeitig sind Begriffe der Alltagssprache weniger abstrakt, das heißt sie erheben keinen universellen Geltungsanspruch über unterschiedliche Kontexte hinweg. „Risiko" beim Glücksspiel bedeutet etwas anderes als „Risiko" beim Betrieb eines Mobilfunkmastes.

Welchen Nutzen können Wissenschaft und Politik in dieser Situation aus der Erforschung der Risikowahrnehmung ziehen?[22] Wahrnehmungsmuster sind keine irrationalen Vorstellungen, sondern in der kulturellen Evolution entstandene und im Alltag bewährte Konzepte, die in vielen Fällen erwartbare Reaktionen von Menschen bei einer Gefahrenwahrnehmung auslösen. Oft sind diese intuitiven Reaktionsweisen unangebracht und sie stehen häufig in keinem Verhältnis zu den wie auch immer berechneten

---

[21] Renn 2005.
[22] Slovic et al. 1982; Streffer et al. 2000, S. 209 ff.; Sjöberg 2001 und 2006.





tatsächlichen Lebens- und Gesundheitsrisiken. Natürliche, selbst steuerbare und in ihren Auswirkungen wenig katastrophal erscheinende Risiken werden systematisch unterschätzt, während die von Menschen erzeugten, als aufgezwungen empfundenen und in der Regel tödlich ausgehenden Gefahren weitgehend überschätzt werden.[23] So sterben in Europa pro Jahr im Schnitt mehrere Tausend Menschen an unhygienischen Lebensmitteln (Bakterien und Pilzbefall), aber nach bestem Wissen der Wissenschaft stirbt niemand an den Folgen chemischer Konservierungsmittel.[24] Dennoch glauben die meisten Menschen, dass chemische Konservierungsmittel viel gefährlicher seien als verdorbene Lebensmittel. Die Erkenntnisse der Risikowahrnehmung können daher jedem Menschen helfen, sich selbst zu beobachten, die eigenen Schwächen der Urteilsbildung zu erkennen und im Wissen um mögliche Folgen des eigenen Handelns und in Anerkennung der eigenen Präferenzen und Vorlieben das eigene Risikoverhalten zu steuern.

Zudem zeigen die empirischen Forschungen zur Risikowahrnehmung auf, dass die grundsätzlichen Mechanismen der mentalen Verarbeitung von Risiken kulturübergreifend wirksam sind.[25] Ihr universeller Charakter über alle Kulturen hinweg ermöglicht eine gemeinsame Orientierung gegenüber Risiken und schafft eine Basis für Kommunikation.[26] Die Wirksamkeit dieser intuitiven Wahrnehmungsprozesse ist zwar abhängig von verinnerlichten Wertvorstellungen und äußeren Situationsumständen; sie bleiben aber bei aller kulturellen Überformung stets präsent und messbar.[27] Diese Erkenntnis ist keine akademische Spitzfindigkeit, sondern unmittelbar relevant für Kommunikation und Konfliktaustragung. Geht man davon aus, dass intuitive Mechanismen der Risikowahrnehmung und -bewertung quasi universelle Züge tragen, die durch soziokulturelle Einflüsse in ihrer Richtung, aber nicht in ihrer Existenz beeinflusst werden können, dann eröffnet sich die Chance auf eine übergreifende gemeinsame Kommunikationsbasis, die man für Kommunikationszwecke über kulturelle Grenzen hinweg zur gegenseitigen Verständigung nutzen kann.





Risikowahrnehmung kann kein Ersatz für rationale Politik sein. Die Politik kann es sich aber weder leisten, noch ist es unter sachlichen Gesichtspunkten sinnvoll, das intuitive Risikoverständnis zu ignorieren oder als irrational abzutun. Es ist durchaus rational, Risiken danach zu beurteilen, wie verschiedene technische Optionen Risiken auf Bevölkerungsgruppen unterschiedlich verteilen, in welchem Maße institutionelle Kontrollmöglichkeiten bestehen und inwieweit Risiken durch freiwillige Vereinbarung übernommen werden. All das sind Aspekte, die in der intuitiven Wahrnehmung große Bedeutung haben. Anders sieht es dann aus, wenn Menschen die Höhe und Tragweite eines Risikos über- oder unterschätzen. Viele Risiken werden schlichtweg verdrängt, weil

23 Slovic 1992; Jungerman/Slovic 1993.
24 Redmond/Griffith 2007.
25 Renn/Rohrmann 2000.
26 Renn 1998.
27 Rohrmann/Renn 2000.



man sich mit ihnen nicht beschäftigen will. Dies gilt vor allem für Risiken, die durch Naturgewalten ausgelöst werden. Sich von verdrängten oder offenkundig falschen Vorstellungen leiten zu lassen, kann kaum eine Rechtfertigung für die Festlegung einer vorausschauenden Umwelt- und Technologiepolitik auf diese Vorstellungen sein. Hier ist die Politik gut beraten, Mut zu zeigen und die besten wissenschaftlichen Ergebnisse für die eigene Entscheidungsfindung zugrunde zu legen, selbst wenn dies unpopulär ist. Wenn Politiker etwa der Verringerung der Risiken durch chemische Lebensmittelzusätze Priorität vor der Verringerung pathogener Gefahren einräumen, dann nehmen sie indirekt in Kauf, dass viele Menschen an verdorbenen Lebensmitteln zu Schaden kommen, ohne dass sich ihr Einsatz zur Verringerung der chemischen Risiken in diesem Bereich nennenswert lohnen würde. Solche Beispiele lassen sich in großer Vielzahl aufführen.

Zu einem rationalen und demokratischen Umgang mit Risiken gehört es, die wissenschaftlichen Expertisen über die möglichen Auswirkungen von Risiken (inklusive der verbleibenden Unsicherheiten) mit den Bewertungen und Gestaltungswünschen der von den Risiken betroffenen Bevölkerung zusammenzufügen und zu einer wissen- und wertorientierten Gesamtpolitik zu integrieren.[28] Dazu bedarf es eines kontinuierlichen Dialogs mit der Bevölkerung, vor allem einer hohen Sensibilität für die Prozesse der Wahrnehmung und Bewertung von Risiken durch die jeweils betroffenen Menschen. Nötig ist aber auch die Entschlossenheit, bei unter- oder überbewerteten Risiken entschieden gegenzusteuern.



2.5 RÜCKWIRKUNGEN AUF VERTRAUEN

In Anbetracht der immer komplexeren Technologien und des Fortschritts der wissenschaftlichen Methoden bei der Bestimmung auch kleinster Mengen schädlicher Substanzen wurde, wie oben dargestellt, die persönliche Risikoerfahrung immer mehr durch Information über Risiken durch Dritte und individuelle Risikokontrolle durch institutionelles Risikomanagement ersetzt. Zunehmend haben wir es mit dem Muster „schleichende Risiken" zu tun. Daraus ergibt sich, dass Menschen sich mehr als je zuvor auf die Glaubwürdigkeit und Aufrichtigkeit derer verlassen (müssen), von denen sie Informationen über Risiken erhalten. Daher ist Vertrauen in institutionelle Leistung maßgebend für die intuitiven Reaktionen auf Risiko. Vertrauen in Kontrolleinrichtungen kann sogar eine negative Risikowahrnehmung ausgleichen und Misstrauen kann Menschen dazu bringen, Risiken abzulehnen, auch wenn sie als gering empfunden werden. In der Tat zeigen manche Forschungsergebnisse ganz klar, dass es eine direkte Wechselbeziehung zwischen gering empfundenem Risiko und öffentlichem Vertrauen gibt und umgekehrt.[29]

[28] Renn 2008.
[29] Siegrist/Cvetkovich 2000; Renn 2008.





Vertrauen kann in sieben Komponenten aufgegliedert werden. Diese sind in Abbildung 1 aufgeführt und erklärt.[30] Vertrauen basiert auf mindestens sechs Bestandteilen, wobei die Nichterfüllung einer Eigenschaft durch hohe Werte auf den anderen Eigenschaften ausgeglichen werden kann. Wenn Objektivität oder Unvoreingenommenheit unmöglich zu erreichen sind, können die Fairness der Botschaft und das Vertrauen in die gute Absicht der Informationsquelle als Ersatz dienen. Auch kann Kompetenz durch Vertrauen ersetzt werden und umgekehrt. Geradlinigkeit ist nicht immer dringend erforderlich, um Vertrauen zu gewinnen, aber andauernde Widersprüche zerstören die allgemeinen Erwartungen und Rollenmodelle für Verhaltensreaktionen.

Abbildung 1: Vertrauenskomponenten

KOMPONENTEN	BESCHREIBUNG
Wahrgenommene Kompetenz	Grad der fachlichen Kompetenz zur Erfüllung des institutionellen Auftrags
Objektivität	keine Voreingenommenheit der Informationen und Leistung wie von anderen wahrgenommen
Fairness	Anerkennung und angemessene Darstellung aller relevanten Standpunkte
Geradlinigkeit	Vorhersehbarkeit von Argumenten und Verhaltensweisen, die auf Erfahrung mit vorhergegangenen Kommunikationsbemühungen basiert
Aufrichtigkeit	Ehrlichkeit und Offenheit
Empathie	Mitgefühl mit den potenziellen Opfern eines Schadens



In Risikodebatten entwickeln sich Vertrauensfragen um Institutionen und deren Vertreter. Die Reaktionen von Personen auf Risiko hängen, unter anderem, von dem Vertrauen ab, das sie in die Institutionen haben, die Risiko verursachen und kontrollieren. Da der Begriff des Risikos impliziert, dass zufällige Ereignisse Unfälle oder Verluste auslösen können, sind Risikomanagementinstitutionen immer gezwungen, ihre Aktivität oder das Fehlen von Aktivität zu rechtfertigen, wenn sie mit einem Unfall konfrontiert werden. Auf der einen Seite können sie Missmanagement vertuschen, indem sie auf die vermeintliche Zufälligkeit des Ereignisses hinweisen (indem sie es als „unvorhersehbar" oder als „höhere Gewalt" bezeichnen), auf der anderen Seite können sie für Ereignisse verantwortlich gemacht werden, für die sie unmöglich im Voraus Schutzmaßnahmen hätten vorsehen können.

Die stochastische Natur von Risiko erfordert eine vertrauensvolle Beziehung zwischen Risikomanager und Risikoträger, da einzelne Ereignisse Fehlleistungen des Managements weder widerlegen noch beweisen; gleichzeitig rufen sie Misstrauen und

[30] Renn/Levine 1988.





Zweifel hervor. Der kleinste Fehler einer Risikomanagementagentur kann ausreichen, um das empfindliche Vertrauensgleichgewicht zu zerstören. Der angeblich laxe Umgang mit Risiko durch private Firmen und Regierungsbehörden war in den meisten Fällen der Auslöser dafür, dass einzelne Personen Initiative ergriffen haben. Je mehr Menschen glauben, dass Risiken nicht angemessen gehandhabt werden (zusätzlich zu der Tatsache, dass sie als ernsthafte Bedrohung empfunden werden), umso höher ist die Wahrscheinlichkeit, dass sie politisch aktiv werden. Es hat sich angesichts der Atomfrage gezeigt, dass die Gegnerschaft in gleichem Umfang angestiegen ist, in dem das Misstrauen in die regulativ tätige Atombehörde gestiegen ist.[31] Negative Einstellungen sind ein notwendiger, aber bei Weitem nicht ausreichender Grund für Verhaltensreaktionen. Das Vertrauen der Öffentlichkeit in die Performanz von Institutionen ist ein weiteres und sogar noch wichtigeres Element für das Auslösen von Verhaltensreaktionen.

Vertrauen aufbauen und gewinnen ist eine vielschichtige Aufgabe, die nicht dadurch erreicht werden kann, dass bestimmte Verfahrensrichtlinien (wie zum Beispiel die Aussage, man verfüge über Einfühlungsvermögen) in mechanischer Weise angewendet werden. Es gibt keine einfache Formel für das Entstehen von Vertrauen. *Vertrauen wächst mit der Erfahrung der Vertrauenswürdigkeit.* Niemand liest eine Broschüre, hört einen Vortrag oder nimmt an einem Gespräch teil, wenn der alleinige Zweck ist, Vertrauen in den Kommunikator aufzubauen. Vertrauen ist das sichtbare Ergebnis erfolgreicher und effektiver Kommunikation über Fragen und Probleme. Je weniger auf das Wort in einer Mitteilung Bezug genommen wird, umso wahrscheinlicher ist es, dass es entweder bestätigt oder überhaupt genannt wird. *Es gibt nur eine allgemeine Regel für das Entstehen von Vertrauen: ein offenes Ohr für die Probleme der Öffentlichkeit zu haben und, wenn erforderlich, sich auf eine dialogorientierte Kommunikation einzulassen.* Information allein ist niemals ausreichend, um Vertrauen aufzubauen oder zu erhalten. Ohne systematische Rückmeldung und Gespräche gibt es keine Atmosphäre, in der Vertrauen wachsen kann.



Risikomanager müssen damit rechnen, dass Risikobewertungen in einer Gesellschaft, in der Wertepluralismus herrscht und politische Handlungen stets unter hohem Rechtfertigungsdruck stehen, oft auf Skepsis oder Misstrauen stoßen. Aussagen zu Risiken sind mehr als andere Aussagen auf Plausibilität (das heißt intuitiv vermittelbare Nachvollziehbarkeit der Gedankengänge) und eben Vertrauen in die Regulierungsgremien angewiesen. Die Regulierung von Risiken kann daher nur im intensiven und verständigungsorientierten Austausch mit der interessierten Öffentlichkeit gelingen.

[31] Slovic 1993.





2.6 OFFENE FORSCHUNGSFRAGEN

Obwohl die Rolle des Vertrauens für die Wahrnehmung und Bewertung von Risiken gut untersucht ist, fehlt es an empirisch gehaltvollen Studien zur Frage nach den Faktoren, die eine vertrauensvolle Zusammenarbeit zwischen risikoregulierenden Institutionen und vor allem zwischen Risikomanagern und den von Risiken betroffenen Bürgerinnen und Bürgern begründen.[32] Wie Vertrauen verloren geht, ist in vielen Fallstudien und auch in systematischen Untersuchungen wissenschaftlich analysiert worden.[33] Was fehlt, ist eine systematische Zusammenschau der Einflussfaktoren und Prozesse, die positiv auf Vertrauensaufbau hinwirken. Ziel sollte es sein, Hilfestellungen für risikoregulierende Institutionen anzubieten, um kontinuierlich Vertrauen zu schaffen und die Vertrauensbasis auch in Zeiten von Krisen aufrechtzuerhalten. Dabei geht es nicht um Kommunikation mit dem Ziel, Inkompetenz und fehlerhaftes Risikoverhalten zu verschleiern oder zu ertragen. Vielmehr heißt „Vertrauensaufbau“, Institutionen so zu gestalten, dass Vertrauen auch verdient werden kann und diese Vertrauenswürdigkeit von außen anerkannt wird.

Wichtig ist dabei, dass die Ergebnisse theoretisch fundiert und empirisch validiert werden. An Anleitungs- und Rezeptbüchern, die auf Common Sense ausgerichtet sind, herrscht kein Mangel. Erforderlich sind professionell durchgeführte empirische Studien, die deutliche Zusammenhänge zwischen institutionellem Verhalten und Vertrauensaufbau belegen.

2.7 LITERATUR

Ad Hoc Kommission 2003
Ad Hoc Kommission der Bundesregierung: „Harmonisierung und Neuordnung der Risikobewertung.“ In: Dies. (Hrsg.): Gutachten an die Bundesregierung,. (Manuskript, Bundesamt für Strahlenschutz), München, 2003.

Beck 1986
Beck, U.: Risikogesellschaft, Frankfurt/Main: Suhrkamp, 1986.

Blackburn 1998
Blackburn, S.: “Trust, Cooperation, and Human Psychology.” In: Braithwaite, V./Levi, M. (Hrsg.): Trust and Governance, New York: Russell Sage, 1998, S. 28-45.

Boholm 1998
Boholm, A.: “Comparative Studies of Risk Perception: A Review of Twenty Years of Research.” In: Journal of Risk Research 1 (1998), Nr. 2, S. 135-163.

---

32 Blackburn 1998; Ad hoc Kommission 2003.
33 Eine Übersicht findet sich in Cvetkovich 1999 und Löfstedt 2005.







Bonß 1996
Bonß, W.: „Die Rückkehr der Unsicherheit. Zur gesellschaftstheoretischen Bedeutung des Risikobegriffs." In: Banse, G. (Hrsg.): Risikoforschung zwischen Disziplinarität und Interdisziplinarität. Von der Illusion der Sicherheit zum Umgang mit Unsicherheit, Berlin: Edition Sigma, 1996, S. 166-184.

Brehmer 1987
Brehmer, B.: "The Psychology of Risk." In: Singleton, W. T./Howden, J. (Hrsg.): Risk and Decisions, Chichester, N. Y.: Wiley, 1987, S. 25-39.

Covello 1983
Covello, V. T.: "The Perception of Technological Risks. A Literature Review." In: Technological Forecasting and Social Change 23 (1983), S. 285-297.

Cvetkovich 1999
Cvetkovich, G.: "The Attribution of Social Trust." In: Cvetkovich, G./Löfstedt, R. (Hrsg.): Social Trust and the Management of Risk, London: Earthscan, 1999, S. 53-61.



Dawes 1988
Dawes, R. M.: Rational Choice in an Uncertain World, New York: Harcourt Brach Jovanovich, 1988.

De Jonge et al. 2007
De Jonge, J./van Kleef, E./Frewer, L./Renn, O.: "Perception of Risk, Benefit and Trust Associated with Consumer Food Choice." In: Frewer, L./Van Trijp, H. (Hrsg.): Understanding Consumers of Food Products, Cambridge: Woodhead, 2007, S. 534-557.

Douglas & Wildavsky 1982
Douglas, M./Wildavsky, A.: Risk and Culture, Berkeley: University of California Press, 1982.

Drottz-Sjöberg 1991
Drottz-Sjöberg, B.-M.: Perception of Risk. Studies of Risk Attitudes, Perceptions, and Definitions, Stockholm: Center for Risk Research, 1991.

Fischhoff 1995
Fischhoff, B.: "Risk Perception and Communication Unplugged: Twenty Years of Process." In: Risk Analysis 15 (1995), Nr. 2, S. 137-145.





Fischhoff et al. 1978
Fischhoff, B./Slovic, P./Lichtenstein, S./Read, S./Combs, B.: "How Safe is Safe Enough? A Psychometric Study of Attitudes toward Technological Risks and Benefits." In: Policy Science 9 (1978), S. 127-152.

Fischhoff et al. 1981
Fischhoff, B./Lichtenstein, S./Slovic, P./Derby, S. L./Keeney, R. L.: Acceptable Risk, Cambridge: Cambridge University Press, 1981.

Gigerenzer/Selten 2001
Gigerenzer, G./Selten, R.: "Rethinking Rationality." In: Gigerenzer, G./Selten, R. (Hrsg.): Bounded Rationality. The Adaptive Toolbox, Boston: MIT Press, 2001.

Gould et al. 1988
Gould, L. C./Gardner, G. Y./DeLuca, D. R./Tieman, A./Doob, L. W./Stolwijk, J. A. J.: Perceptions of Technological Risk and Benefits, New York: Russel Sage Foundation, 1988.

IRGC 2005
International Risk Governance Council (IRGC) (Hrsg.): White Paper on Risk Governance. Towards an Integrative Approach, (Autoren: Renn, O. /Graham, P.), Geneva: International Risk Governance Council, 2005.

Jaeger et al. 2001
Jaeger, C. C./Renn, O./Rosa, E. A./Webler, T.: Risk, Uncertainty and Rational Action, London: Earthscan, 2001.

Jungermann 1982
Jungermann, H.: „Zur Wahrnehmung und Akzeptierung des Risikos von Großtechnologien." In: Psychologische Rundschau 23 (1982), Nr. 3, S. 217-238.

Jungermann 1986
Jungermann, H.: "The Two Camps of Rationality." In: Arkes, H. R./Hammond, K.R. (Hrsg.): Judgment and Decision Making: An Interdisciplinary Reader, Cambridge: Cambridge University Press, 1986, S. 465-471.

Jungermann et al. 2005
Jungermann, H./Pfister, H.-R./Fischer, K.: Die Psychologie der Entscheidung, 2. Aufl. Heidelberg: Elsevier Spektrum Akademischer Verlag, 2005.







Jungermann/Slovic 1993a
Jungermann, H./Slovic, P.: „Die Psychologie der Kognition und Evaluation von Risiko." In: G. Bechmann (Hrsg.): Risiko und Gesellschaft. Grundlagen und Ergebnisse interdisziplinärer Risikoforschung, Opladen: Westdeutscher Verlag, 1993, S. 167-207.

Jungermann/Slovic 1993b
Jungermann, H./Slovic, P.: „Charakteristika individueller Risikowahrnehmung." In: Bayerische Rückversicherung (Hrsg.): Risiko ist ein Konstrukt. Wahrnehmungen zur Risikowahrnehmung, München: Knesebeck, 1993, S. 90-107.

Kasperson et al. 2003
Kasperson, J. X./Kasperson, R. E./Pidgeon, N./Slovic, P.: "The Social Amplification of Risk: Assessing Fifteen Years of Research and Theory." In: Pidgeon, N./Kasperson, R. E./Slovic, P. (Hrsg.): The Social Amplification of Risk, Cambridge: Cambridge University Press, 2003, S. 13-46.

Kraus et al. 1992
Kraus, N./Malmfors, T./Slovic, P.: "Intuitive Toxicology: Expert and Lay Judgments of Chemical Risks." In: Risk Analysis 12 (1992), S. 215-232.



Löfstedt 2005
Löfstedt, R.: Risk Management in Post Trust Societies. Palgrave-Macmillan, London, 2005.

Machlis/Rosa 1990
Machlis, E./Rosa, E.: "Desired Risk: Broadening the Social Amplification of Risk Framework." In: Risk Analysis 10 (1990), S. 161-168.

Miller 1985
Miller, S.: Perception of Science and Technology in the United States, (Manuscript for the U.S. Academy of Sciences, National Research Council), Washington, D.C., 1985.

National Research Council 1989
National Research Council (NRC): Improving Risk Communication, Washington, D.C.: National Academy Press, 1989.

OECD 2002
OECD: Guidance Document on Risk Communication for Chemical Risk Management, Paris: OECD Press, 2002.





Okrent 1998
Okrent, D.: "Risk Perception and Risk Management: On Knowledge, Resource Allocation and Equity." In: Reliability Engineering and Systems Safety 59 (1998), S. 17-25.

Pidgeon et al. 1992
Pidgeon, N. F./Hood, C. C./Jones, D. K. C./Turner, B. A./Gibson, R.: "Risk Perception." In: Royal Society Study Group (Hrsg.): Risk Analysis, Perception, and Management, London: The Royal Society, 1991, S. 89-134.

Renn 1989
Renn, O.: „Risikowahrnehmung – Psychologische Determinanten bei der intuitiven Erfassung und Bewertung von technischen Risiken." In: Hosemann, G. (Hrsg.): Risiko in der Industriegesellschaft, Nürnberg: Universitätsverlag, 1989, S. 167-192.

Renn 1998
Renn, O.: "The Role of Risk Perception for Risk Management." In: Reliability Engineering and System Safety 59 (1998), S. 49-61.



Renn 2004
Renn, O.: "Perception of Risks." In: The Geneva Papers on Risk and Insurance 29 (2004), Nr. 1, S. 102-114.

Renn 2005
Renn, O.: "Risk Perception and Communication: Lessons for the Food and Food Packaging Industry." In: Food Additives and Contaminants 22 (2005), Nr. 10, S. 1061-1071.

Renn 2008
Renn, O.: Risk Governance. Coping with Uncertainty in a Complex World, London: Earthscan, 2008.

Renn/Levine 1989
Renn, O./Levine, D.: "Trust and Credibility in Risk Communication." In: Jungermann, H/Kasperson, R. E./Wiedemann P. M. (Hrsg.): Risk Communication, Jülich: Forschungszentrum Jülich, 1989, S. 51-82.

Renn/Rohrmann 2000
Renn, O./Rohrmann, B.: "Cross-Cultural Risk Perception Research: State and Challenges." In: Renn, O./Rohrmann, B. (Hrsg.): Cross-Cultural Risk Perception. A Survey of Empirical Studies, Dordrecht,Boston: Kluwer, 2000, S. 211-233.





Rohrmann/Renn 2000
Rohrmann, B./Renn, O.: „Risk Perception Research – An Introduction." In: Renn, O./ Rohrmann, B. (Hrsg.): Cross-Cultural Risk Perception. A Survey of Empirical Studies. Dordrecht, Boston: Kluwer, 2000, S. 11-54.

Ross 1977
Ross. L. D.: "The Intuitive Psychologist and His Shortcomings: Distortions in the Attribution Process." In: Berkowitz, L. (Hrsg.): Advances in Experimental Social Psychology (Heft 10), New York: Random House, 1977, S. 173-220.

Siegrist/Cvetkovich 2000
Siegrist, M./Cvetkovich, G.: "Perception of Hazards: The Role of Social Trust and Knowledge." In: Risk Analysis 20 (2000), S. 713-719.

Sjöberg 1997
Sjöberg, L.: "Explaining Risk Perception: An Empirical and Quantitative Evaluation of Cultural Theory." In: Risk, Decision, and Policy 2 (1997), S. 113-130.

Sjöberg 1999a
Sjöberg, L.: "Risk Perception in Western Europe." In: Ambio 28 (1999), Nr. 6, S. 543-549.

Sjöberg 1999b
Sjöberg, L.: "Consequences of Perceived Risk." In: Journal of Risk Research 2 (1999), S. 129-149.

Sjöberg 2001
Sjöberg, L.: "Political Decisions and Public Risk Perception." In: Reliability Engineering & System Safety 72 (2001), S. 115-123.

Sjöberg 2006
Sjöberg, L.: "Rational Risk Perception: Utopia or Dystopia?" In: Risk Research 9 (2006), Nr. 6, S. 683-696.

Slovic 1987
Slovic, P.: "Perception of Risk." In: Science 236 (1987), S. 280-285.

Slovic 1992
Slovic, P.: "Perceptions of Risk: Reflections on the Psychometric Paradigm." In. Krimsky, S./Golding, D. (Hrsg.): Social Theories of Risk, Westport: Praeger, 1992, S. 153-178.





Slovic 1993
Slovic, P.: "Perceived Risk, Trust, and Democracy." In: Risk Analysis 13 (1993), S. 675-682.

Slovic/Fischhoff 1982
Slovic, P./Fischhoff, B.: "How Safe is Safe Enough? Determinants of Perceived and Acceptable Risk." In: Gould, L. C./Walker, W. (Hrsg.): Too Hot to Handle, New Haven: Yale University Press, 1982, S. 156-189.

Slovic et al. 1981
Slovic, P./Fischhoff, B./Lichtenstein, S.: Perceived Risk: Psychological Factors and Social Implications, (Proceedings of the Royal Society, A376), London: Royal Society, 1981, S. 17-34.

Slovic et al. 1982
Slovic, P./Fischhoff, B./Lichtenstein, S.: "Why Study Risk Perception?" In: Risk Analysis 2 (1982), S. 83-94.

Streffer et al. 2000
Streffer, C./Bücker, J./Cansier, A./Cansier, D./Gethmann, C. F./Guderian, R./Hanekamp, G./Henschler, D./Pöch, G./Rehbinder, E./Renn, O./Slesina, M./Wuttke, K.: Umweltstandards. Kombinierte Expositionen und ihre Auswirkungen auf den Menschen und seine Umwelt, Heidelberg, Berlin: Springer, 2000.

Slovic et al. 2002
Slovic, P./Finucane, M. L./Peters, E./MacGregor, D. G.: "The Affect Heuristic." In: Gilovich, T./Griffin, D./Kahneman, D. (Hrsg.): Intuitive Judgment: Heuristics and Biases, Cambridge/Boston: Cambridge University Press, 2002, S. 397-420.

Tversky 1972
Tversky, A.: "Elimination by Aspects: A Theory of Choice." In: Psychological Review 79 (1972), S. 281-299.

Tversky/Kahneman 1981
Tversky, A./Kahneman, D.: "The Framing of Decisions and the Psychology of Choice." In: Science 211 (1981), S. 453-458.

Vlek/Stallen 1981
Vlek, C. A. J./Stallen, P. J.: "Judging Risks and Benefits in the Small and in the Large." In: Organizational Behavior and Human Performance 28 (1981), S. 235-271.



Wiedemann 1993
Wiedemann, P. M.: „Tabu, Sünde, Risiko: Veränderungen der gesellschaftlichen Wahrnehmung von Gefährdungen." In: Bayerische Rückversicherung (Hrsg.): Risiko ist ein Konstrukt. Wahrnehmungen zur Risikowahrnehmung, München: Knesebeck, 1993, S. 43-67.

Wildavsky 1990
Wildavsky, A.: "No Risk is the Highest Risk of All." In: Glickman, T. S./Gough, M. (Hrsg.): Readings in Risk. Resources for the Future, Washington, D.C., 1990, S. 120-127.

Wildavsky/Dake 1990
Wildavsky A./Dake, K.: "Theories of Risk Perception: Who Fears What and Why?" In: Daedalus 119 (1990), S. 41-60.

Zwick 2006
Zwick, M. M.: "Risk as Perceived and Evaluated by the General Public." In: Ammann, W. J./Dannenmann, S./Vulliet, L. (Hrsg.): RISK21 – Coping with Risks Due to Natural Hazards in the 21st Century, London: Taylor & Francis, 2006, S. 89-100.






3 TECHNIKSICHERHEIT UND SICHERHEITSKULTUREN

GERHARD BANSE

3.1 BEDEUTUNGSVIELFALT, WERTHAFTE IMPLIKATIONEN UND PRAKTISCHE AMBIVALENZEN VON „SICHERHEIT“

„Sicherheit“ ist ein zentrales Konzept in Gesellschaft, Wissenschaft und Technik. Geprägt wird dieses Konzept von unterschiedlichen Begriffsauffassungen, Kommunikationsstrategien und kulturellen Aspekten. Individuell gewendet, schlägt es sich in einem zunehmenden Sicherheitsbedürfnis nieder; gesellschaftlich spiegelt es sich beispielsweise in einer forcierten Sicherheitspolitik wider. Sicherheit ist ein Versprechen, das gerade in modernen, hochtechnisierten Gesellschaften zunehmend versucht wird, über Technik einzulösen. Die Erwartung an und die Herstellung von Sicherheit in allen Bereichen der Lebenswelt sind allgegenwärtig. Durch diese Ubiquität ist Sicherheit ein zentraler Gegenstand wissenschaftlicher Forschung. Allerdings: Untersuchungen von Franz-Xaver Kaufmann haben gezeigt, dass „Sicherheit“ ein schillernder Begriff ist, denn das Wort „Sicherheit“ wird im Deutschen in mindestens drei Bedeutungen verwendet:[1]

a) „Sicherheit“ als Geborgenheit;
b) „Sicherheit“ als Selbstsicherheit;
c) „Sicherheit“ als Systemsicherheit (das heißt herstellbare, berechenbare Mittel für beliebige Zwecke).

Die Sicherheit technischer Handlungsvollzüge und technischer Hervorbringungen als weitgehender Ausschluss oder als bewusstes Handling von (möglichen) Gefährdungen für „Schutzgüter“ nimmt in den handlungsleitenden Wertvorstellungen technischer

1 Vgl. Kaufmann 1973, S. 67ff.



Welterzeugung einen herausragenden Platz ein.[2] Dabei geht es sowohl um den Erhalt des erreichten „status quo" unter dynamischen „Randbedingungen" als auch – oder vor allem (?) – um dessen Verbesserung und Erhöhung durch ursachen- und wirkungsorientierte Maßnahmen.[3] Zu berücksichtigen sind jedoch zwei Einsichten: Erstens bezieht sich „Sicherheit" auf etwas Zukünftiges, auf einen Zusammenhang zwischen einer gegenwärtigen Lage und dem Ausschluss eines zukünftigen Schadensereignisses; zweitens erfasst „Sicherheit" den Ausschluss eines zukünftig nur möglichen Ereignisses, dessen Eintritt weder gewiss noch unmöglich ist. Erkenntnisungewissheiten über das Auftreten bzw. Nichtauftreten derartiger Gefahren-, Versagens- oder Schadensmöglichkeiten begleiten die technische Welterzeugung von Anfang an, was unter anderem als Differenz zwischen Handlungsziel und Handlungsergebnis, dem Eintreten zufälliger Ereignisse oder dem Auftreten nicht-intendierter Folgen erfahren wurde.




2 Vgl. zum Beispiel VDI 1991. – „technische Welterzeugung" bedeutet zum einen die technisch vermittelte (instrumentierte) Schaffung (das heißt Generierung, Veränderung, Gestaltung, Zerstörung) von Lebenswelt, zum anderen die Hervorbringung und Nutzung der Welt des „Technischen", der Artefakte. Sie umfasst zugleich unterschiedlichste Bereiche: die Erzeugung „realtechnischer Welten" mittels handwerklicher, industrieller und landwirtschaftlicher Produktion, die „Konstruktion" von „Informationswelten" mittels moderner Kommunikationstechnologien und den Aufbau „virtueller Realitäten" mittels fortgeschrittener Informationstechnologien. Eingeschlossen darin sind die – den Bereich des nur Denkbaren bereits überschrittenen – Möglichkeiten der zielgerichteten Manipulation des genetischen Materials durch gentechnologische Prozeduren, des Omnizids angesichts der vorhandenen militärischen Vernichtungstechnik und des ökologischen Kollaps' infolge „vernünftige" (das heißt auch: zukunftsfähige) Maßstäbe überschreitender Eingriffe bzw. Einträge in die natürlichen Bedingungen gesellschaftlicher Existenz und Entwicklung. Zu berücksichtigen ist zudem, dass es nicht allein nur um die „Folgen" oder „Wirkungen" dieser technisch generierten bzw. vermittelten Welten geht, sondern dass der Gesamtprozess der Welterzeugung vom ideellen Entwurf und der systematischen Gestaltung über die Herstellung und vielfältige („sichere") Nutzung bis hin zu den verschiedenartigsten Konsequenzen für Individuum, Gesellschaft, Natur und „Weltbild" zu thematisieren ist. Eine Betrachtung des „Erzeugens" von Welt, ihrer Dynamik, ihres Werdens und Vergehens durch und mittels Technik impliziert – im Gegensatz zu einer mehr statisch ausgerichteten „Seinsbetrachtung" – die Einbeziehung der Zeitkomponente. Neben Zeitpunkt (zum Beispiel des Auf- bzw. Eintretens interessierender Ereignisse oder Situationen sowie von Entscheidungen, Handlungen oder Unterlassungen), Zeitdauer (zum Beispiel von Wahrnehmungen, Handlungsvollzügen oder Handlungsfolgen) und Zeitfenster (vor allem als zeitlich – bewusst oder unbewusst – begrenzter „Ausschnitt" technisch erzeugter oder beeinflusster „Welt") bekommen auch solche Kategorien wie (Nicht-)Überschaubarkeit und (Nicht-)Beeinflussbarkeit von Abläufen in einem Zeitintervall, (Ir-)Reversibilität von Eingriffen und Wirkungen, Kontingenz des Geschehens sowie (Selbst-)Referenz und Rückkopplung von Ereignissen erkenntnis- und handlungsleitende Relevanz. Damit werden dann nicht nur auf je spezifische Weise ökonomische, ökologische, politische, psychische, soziale und kulturelle Fragestellungen aufgeworfen bzw. tangiert, sondern auch unterschiedlichste kognitive und normative Probleme sichtbar gemacht, die etwa von den individuellen Voraussetzungen zielgerichteten kreativen „Erzeugens" (auch von Sicherheit!) und der Art der dem technischen Handeln zugrunde liegenden Wissensformen (auch hinsichtlich Sicherheit!) über Bewertungs- und Selektionskriterien für mögliche technische Realitäten einschließlich sich darin äußernder Rationalitätstypen bis hin zu Sinn- und Orientierungsfragen in einer „zersplitterten Welt" (vgl. Holz 1992) reichen. (Vgl. näher dazu Banse/Friedrich 1996).

3 „Gefahr" bedeutet eine Lage, „in der bei ungehindertem Ablauf des Geschehens ein Zustand oder ein Verhalten mit hinreichender Wahrscheinlichkeit zu einem Schaden für die Schutzgüter der [...] Sicherheit [...] führen würde" (Drews/Wacke/Vogel 1986, S. 220).



Man kann davon ausgehen, dass das Streben nach Sicherheit – verstanden als Abwesenheit von Gefahr, von Ungewissheit, von Kontingenz usw. – ein menschliches Grundbedürfnis ist, eine „Wertidee hochdifferenzierter Gesellschaften" (wie von Kaufmann herausgearbeitet)[4]. Überlegungen zu Sicherheitskulturen lassen sich der Erreichung dieses Ziels, dem „Gewinnen" bzw. „Herstellen" von Sicherheit, mithin der „Überwindung" von Unsicherheit[5] zuordnen. (Das kann sowohl bedeuten, dass Gefahren tatsächlich abgeschafft bzw. reduziert werden, als auch, dass sich veränderte Sicherheitsüberzeugungen oder gar -fiktionen im Sinne der – wie es Wolfgang Bonß genannt hat – „Umdefinition und Verlagerung von Ungewissheit"[6] herausbilden.)

Das „Herstellen" von Sicherheit ist in diesem Verständnis Überwindung nicht-handhabbarer Zusammenhänge (zum Beispiel in Form von Kontingenz und Ambiguität), deren Überführung in handhabbare, strukturierte, „systemische" Formen, womit




4 Kaufmann 1973; vgl. auch Bachmann 1991; Robbers 1987.

5 Damit ist nicht ausgeschlossen, dass es nicht nur individuell, sondern auch gesellschaftlich sowohl unterschiedliche Wahrnehmungen von Unsicherheit als auch Strategien zur Sicherheitsherstellung gibt; vgl. Bonß 1997.

6 Bonß 1997, S. 23.



– um nochmals Bonß zu zitieren – „aus einem Universum denkbarer Möglichkeiten bestimmte Möglichkeiten als handlungsrelevant ausgewählt, andere hingegen als irrelevant ausgeblendet werden".[7] Solche Aktivitäten wie das Aufweisen eines möglichen Ereignis- oder zukünftigen Zustandsspektrums, das Ermitteln von Eintrittshäufigkeiten, das Ableiten von Erwartungswerten, das Abwägen von Aufwand und Nutzen oder die Kalkulation von „Gewinnen" und „Verlusten" (nicht allein im monetären Sinne) dienen der zielgerichteten Einflussnahme und produktiven Handhabung („Beherrschung") von Unbestimmtheit. „Mehrdeutigkeit" wird auf diese Weise nicht in erster Linie in „Eindeutigkeit" überführt, „Zufälligkeit" nicht auf „Notwendigkeit" zurückgeführt – obwohl das nicht ausgeschlossen ist –, sondern als „eindeutig" und „wohlbestimmt" gefasst und behandelt. Auf diese Weise wird vor allem ein methodischer Gewinn erzielt, erlaubt doch diese „Idealisierung" und „Reduzierung" (die immer auch eine „Ausblendung" ist!) die Anwendung spezifischer Methoden und ermöglicht (erst) einen rationalen Zugriff auf Situationen unvollständiger Information.[8]

In diesem Kontext ist letztlich darauf zu verweisen, dass die „Herstellung" von Sicherheit in sich ambivalent ist: Auf der einen Seite wird die Bandbreite und Variationsvielfalt des zukünftig Möglichen eingeschränkt (was einer faktischen Beschränkung von Freiheitsgraden und Wahlmöglichkeiten bedeutet); andererseits ist gerade die Schaffung und Gewährleistung dieser Sicherheit entscheidende Grundlage für die Stabilisierung von Verhalten und die Herstellung von Planungsmöglichkeit.[9]



3.2 ERWEITERUNG UND NEUORIENTIERUNG DES VERSTÄNDNISSES VON „TECHNIKSICHERHEIT" IN RICHTUNG EINES „UNBESTIMMTHEITS-PARADIGMAS"

Unter den oben genannten „Schutzgütern" werden hier in erster Linie körperliche Unversehrtheit, Lebenserhaltung des einzelnen Menschen sowie Lebenserhaltung der Menschheit, aber auch Unversehrtheit bzw. Erhaltung der sogenannten natürlichen Umwelt des Menschen sowie der technischen Systeme selbst verstanden. Hinzu kommt die ursachen- wie wirkungsbezogene Minimierung von Risiken (Schadensumfang und Eintrittswahrscheinlichkeit), und zwar bezogen auf das Betriebs-, das Versagens- und das Missbrauchsrisiko.[10] Dieser „Leistungskatalog" verweist auch darauf, dass Technik-

---

7 Bonß 1997, S. 24.

8 Vgl. näher Banse 2002b; vgl. auch Banse 1996.

9 Vgl. Lippert/Prüfert/Wachtler 1997, S. 18; aus einer anderen Perspektive vgl. auch Grunwald 1997.

10 Damit wird über eine stärker „technikinterne" Sicht auf (Technik-)Sicherheit hinaus, die vor allem den technischen Versagensfall, seine Ursachen und seine mögliche Verhinderung thematisiert, auf dessen mögliche „externe", das „Unmittelbar-Technische" überschreitende Effekte fokussiert. – Als funktionierender (das heißt als gelingender bzw. gelungene) Technik ist ihr (allerdings in einem etwas anderen Sinne) Sicherheit inhärent, da sie den wiederholten erfolgreichen (das heißt „sicheren") Vollzug technischer „Regeln" repräsentiert (zum hier unterstellten Regelverständnis vgl. Grunwald 2009). Im Rahmen dieses Verständnisses sind etwa technische Pannen oder Versagensfälle als Fälle des Misslingens des Regelvollzugs interpretierbar. – Wie die Darlegungen von Ortwin Renn in diesem Band belegen, besteht ein enger Zusammenhang zwischen (allgemeiner) Sicherheits- und Risikoforschung. Meines Erachtens handelt es sich dabei um zwei unterschiedliche Betrachtungsperspektiven mit je eigenen und spezifischen Konzeptualisierungen.





sicherheit im eingeführten Verständnis nicht nur technische, sondern auch sogenannte „nicht-technische" Anteile besitzt[11] und nicht durch Natur- und Technikwissenschaften allein, sondern nur durch Einbeziehung von Sozial- und Geisteswissenschaften realisiert werden kann.

Technische Sicherheit und Beherrschbarkeit von Technik sowie Wissen über Schadenserwartungen und Folgewirkungen werden auf vielfältige Weise angestrebt. Bei technisch bedingten Unfällen wird vor allem der Verlust von Kontrolle über solche Zusammenhänge erfahren, deren Beherrschbarkeit als gegeben angesehen wurde. Bisher nicht bekannte oder unberücksichtigt gebliebene Eigenschaften und Verhaltensweisen von Systemen und ihren Elementen, Randbedingungen für Funktionsfähigkeit und Betriebssicherheit, ungeprüfte oder unüberprüfbare Annahmen hinsichtlich Funktionszusammenhängen oder Belastungsfähigkeiten (etwa in extremen Situationen) sowie Inkompatibilitäten im Mensch-Maschine-System werden im Unfall schlagartig aktualisiert. Deshalb wird seit Längerem durch unterschiedliche Wissenschaftsdisziplinen und mit verschiedenen Methoden Ursachen, Wirkungen und Wahrscheinlichkeiten von Havarien und Schadensfällen sowie ihren Verläufen ebenso nachgegangen wie Möglichkeiten ihrer Verhinderung bzw. Limitierung.

Aufbauend auf dem erreichten Stand der (Allgemeinen) Sicherheitsforschung, die sich vor allem auf Erkenntnisse der Technikwissenschaften (zum Beispiel der Sicherheitswissenschaft), der Arbeits- und Ingenieurpsychologie sowie weiterer Arbeitswissenschaften stützt und vorrangig auf den Ebenen Technikgestaltung sowie Organisation und Management ansetzt, bildet sich derzeit ein breiteres Sicherheitsverständnis heraus, dass in stärkerem Maße als in der ingenieurtechnischen Forschung bislang üblich kulturelle Aspekte einschließt. Rückblickend auf die (technische) Sicherheitsforschung kann festgestellt werden, dass sich mit der Ausweitung des Forschungsfeldes (komplexere Erfassung von Zusammenhängen und Wechselwirkungen, Einbeziehung von Mensch-Technik-Interaktionen, Verständnis von Technik als sozio-technischem und kulturellem „Phänomen") zugleich der Bereich der involvierten wissenschaftlichen Disziplinen über die Technik- und die Wirtschaftswissenschaften (sowie die mit ihnen verbundenen Naturwissenschaften und Mathematik) hinaus ständig erweitert hat und gegenwärtig

---

[11] Dass diese Unterscheidung eigentlich irreführend ist, wird später deutlich (gemacht).





auch viele sozial-, kultur- und geisteswissenschaftliche Disziplinen betrifft. Erwartet (und möglich) ist dadurch ein Zugewinn an Techniksicherheit bzw. – andersherum – eine Reduzierung von Gefahrenpotenzialen.

Technikphilosophie beispielsweise ist, bezogen auf „sichere" Technik, einerseits mit der Klärung grundlegender Begrifflichkeiten (etwa Facetten des Sicherheitsverständnisses), Argumentationen und Begründungsverfahren sowie mit dem Herausarbeiten impliziter Bedeutungsgehalte und Prämissen befasst. Damit schließt sie sowohl an die Linguistik als auch an die Kulturwissenschaften an. Andererseits formuliert sie spezifische Standards und identifiziert mögliche Kriterien, die bei der Beurteilung von (Technik-)Sicherheit und dem praktischen Umgang mit technisch bedingten Gefährdungen zugrunde zu legen sind (bzw. zugrunde gelegt werden sollten). Der normative Aspekt technischer Sicherheit zeigt sich darin, dass das, was als wünschenswerte bzw. nicht wünschenswerte Folgen technischen Handelns bewertet, was als adäquate bzw. nicht adäquate gesellschaftliche Antwort auf technisch bedingte Problemsituationen betrachtet und welcher Bereich möglicher Gefährdungen wahrgenommen bzw. ausgeblendet wird, von Wert- und Normvorstellungen abhängt – die immer auch kulturell geprägt sind.



Es war – und ist teilweise noch – der Anspruch der Risikoforschung, Unsicherheit und Ungewissheit beseitigen sowie Sicherheit und Gewissheit herzustellen bzw. wenigstens zu deren Herstellung beitragen zu können. Und: Es lassen sich vielfältige Ergebnisse vorweisen, die technische Lösungen in der Vergangenheit sicherer, zuverlässiger, gefahrloser werden ließen, Ergebnisse, die zur Reduzierung, Limitierung oder gar Vermeidung von Risiken beitrugen. Damit einher ging die Ausprägung der Überzeugung (des Paradigmas), sich zwar nur allmählich, aber doch zielgerichtet und kontinuierlich der „absoluten" Sicherheit bis auf ein – vernachlässigbares – Restrisiko zu nähern bzw. nähern zu können. Aaron Wildavsky nannte das die „Suche nach einer fehlerlosen Risikominimierungsstrategie".[12] Vernachlässigt wurde, dass viele Überlegungen auf hypothetischen und Modellannahmen sowie auf einer eingeschränkten Datenbasis grün-

[12] Wildavsky 1984.





deten, dass sich das Geschehen in der technischen Welt nicht nur nach Berechnungen und Simulationen richtet und das zukünftige „Verhalten" von Mensch-Technik-Systemen nur bedingt prognostizierbar ist. Beinahe-Unfälle, Pannen, Havarien oder gar Katastrophen waren das Ergebnis.[13] Hinzu kamen Einsichten einzelner Disziplinen (verwiesen sei lediglich auf Psychologie und Arbeitswissenschaften), die die Einlösbarkeit des „Sicherheits-Paradigmas" infrage stellten und – in zunehmendem Einklang mit anderen Wissenschaften (etwa der Soziologie, Philosophie, den Rechtswissenschaften und der Ökonomie) – neue Denkanstöße und Lösungsmöglichkeiten für die Behandlung technischer Risiken und die „Erzeugung" von (Technik-)Sicherheit nicht nur forderten, sondern (wenn auch erst ansatzweise) vorlegten.[14] Diese Neuorientierung, diese Änderung der Forschungsperspektive schließt meines Erachtens ein:

- „Zunächst einmal muß die nach wie vor vorherrschende Fixierung auf das Ideal vollständiger Sicherheit relativiert werden".[15]
- Sodann ist „ein Wechsel von Eindeutigkeits- zu Uneindeutigkeitsorientierungen" für die Einschätzung der tatsächlichen Möglichkeiten der Verfahren zur Sicherheitsherstellung erforderlich.[16]
- Schließlich ist – auf methodologischer und wissenschaftstheoretischer Ebene – der Status von Risikowissen vor allem zwischen der naturwissenschaftlich konstatierten bzw. geforderten „Objektivität" und dem sozialwissenschaftlich zugeschriebenen „Konstruktcharakter" genauer aufzuklären.[17]




Dieser Perspektivenwechsel kann die allmähliche Ausprägung eines „Unbestimmtheits-Paradigmas" genannt werden, für das der bewusste und (ein-)geplante Umgang mit Unsicherheiten und Ungewissheiten der Technik infolge der Einsicht in deren prinzipielle Irreduzibilität charakteristisch ist.[18]

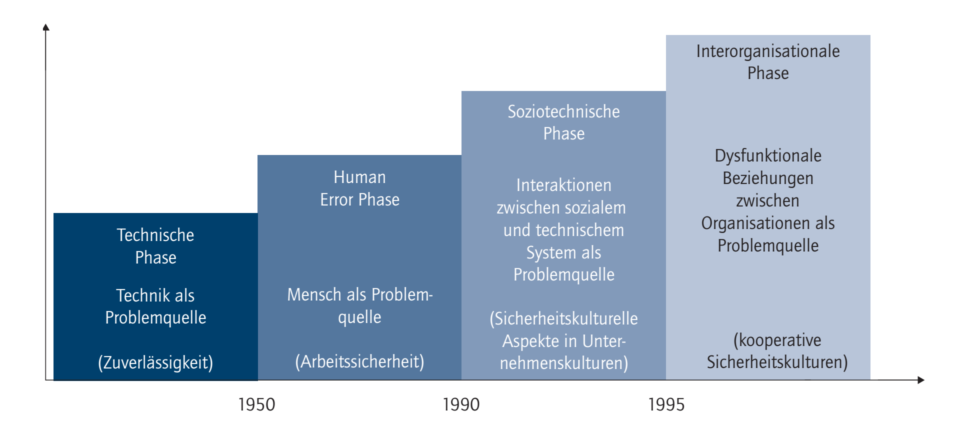
---

13 Vgl. etwa Perrow 1989; vgl. auch Hofmann 2008.
14 Vgl. etwa Dörner 1989; Gethmann/Klöpfer 1993; Guggenberger 1987; Perrow 1989; Wehner 1992.
15 Bonß 1997, S. 35.
16 Vgl. Bonß 1997, S. 36.
17 Vgl. auch Frederichs/Bechmann 1997.
18 Eigentlich müsste – in Anlehnung an Bonß – hierbei von „uneindeutigen" Unbestimmtheiten gesprochen werden, da es bei „eindeutigen" Unbestimmtheiten – im Bereich der Technik eher die Ausnahme denn die Regel – „um geschlossene Systeme mit präzise definierten Rahmenbedingungen und Ergebnissen geht, die klare Prognosen und sichere Aussagen erlauben" (Bonß 1997, S. 29).





Abbildung 1: Ausweitung des Techniksicherheits-Verständnisses[19]






Das oben genannte, ständig sich erweiternde Sicherheitsverständnis deuten Torsten Büttner, Babette Fahlbruch und Bernhard Wilpert in Abbildung 1 an (siehe oben). Dies korrespondiert auf interessante Weise mit einem Technikverständnis, das sich in den letzten Jahren erweitert hat. Geht man in Anlehnung an einen Vorschlag von Günter Ropohl von (a) engen, (b) mittelweiten (mittleren) und (c) weiten Technikverständnissen aus, so gibt es im Bereich (b) unter anderem folgende Differenzierungen:[20]

1. Mit dem Konzept des *Mensch-Maschine-Systems* werden Verwendungs- bzw. Nutzungszusammenhänge auf der Ebene des Individuums einbezogen: Technik ist stets in menschliche Handlungsvollzüge eingebunden.[21]

---

19 Nach Büttner/Fahlbruch/Wilpert 1999, S. 30.

20 Vgl. näher dazu Banse 2002a, S. 26ff.

21 Der Anspruch der Gestaltung von Mensch-Technik-Systemen, der vor allem seitens der Arbeitswissenschaften und der Ingenieurpsychologie formuliert wurde, besteht generell in der „Rehabilitierung" des Menschen in technisch vermittelten und unterstützten Arbeitsprozessen, im „Detail" in der Gestaltung optimaler, „systemischer" Mensch-Maschine-Beziehungen unter Berücksichtigung der je unterschiedlichen Leistungsfähigkeit und Leistungsparameter der menschlichen und der technischen „Komponente" sowie vor allem ihrer „Schnittstellen" („interfaces") und Kopplungsbereiche. Helmut Reuter und Theo Wehner umreißen die Situation wie folgt: „Sichere Gesamtzustände unter Beteiligung von Menschen haben andere Eigenschaften als technische Apparate. Das Hinzutreten des Menschen in diesen Systemzusammenhang ist wesentlich mit Schuld an den veränderten Eigenschaften. Unter Einfluß menschlichen Handelns werden die Systemzustände prinzipiell unvorhersagbar und selbst in ihrer Wahrscheinlichkeitsberechnung problematisch" (Reuter/Wehner 1996, S. 94). Worum es unter diesen Bedingungen geht, ist nicht die Strategie einer möglichst konsequenten Trennung von Mensch und Maschine sowie die technische „Bekämpfung" des „Feindes" Mensch als „Sicherheitsrisiko Nr. 1" (das würde weitgehend dem klassischen Risikomanagement entsprechen!), sondern sowohl die Verbesserung der Handlungskompetenz (indem zum Beispiel der Arbeitsort zum Lernort aufgewertet wird) als auch Veränderungen in der Funktionsteilung zwischen Mensch und Technik, die sowohl den jeweiligen „Stärken" und „Schwächen" als auch möglichen Ambiguitäten Rechnung trägt.

2. Werden darüber hinaus soziale (vor allem sozio-ökonomische) Zusammenhänge sowohl der Entstehung wie auch der Verwendung bzw. Nutzung technischer Sachsysteme einbezogen, wird Technik als *„sozio-technisches System"* (Ropohl) unterstellt.[22] „Technik" bezeichnet nicht nur die von Menschen gemachten Gegenstände (technische Sachsysteme, „Artefakte") selbst, sondern schließt auch deren Entstehungs- und Verwendungszusammenhänge („Kontexte") ein (also das „Gemacht-Sein" und das „Verwendet-Werden"). Vielfach werden jedoch vorrangig einerseits der Entstehungszusammenhang thematisiert, andererseits die sozialen Bedingungen und „Kontexte" auf sozioökonomische reduziert (zum Beispiel „Markt", „Macht").
3. *Technik als Kulturprodukt* („kultivierte Technik") zu verstehen, geht davon aus, dass Technik „ihren Einsatz und ihren alltäglichen Gebrauch [...] in einem soziokulturellen Kontext, im Kontext kollektiver Interpretationen und Deutungen" findet.[23] Ausgangspunkt ist die Einsicht, dass technische Objekte keinesfalls notwendigerweise so und nicht anders, wie sie uns allgegenwärtig sind, das heißt aus autonomen technischen Bedingungen, in den Alltag gelangen. Technische Sachsysteme sind in ihrer Entstehung wie in ihrer Verwendung Ausdruck eigener wie fremder („eingebauter") Absichten und Zwecke. Die Hervorbringung, Implementierung und Diffusion technischer Lösungen wird über die Kultur der sie „tragenden" Menschen erheblich beeinflusst, indem diese zum Beispiel für die Realisierung von Zwecken genutzt oder nicht genutzt (abgelehnt), Modifizierungen, Nachbesserungen und Anpassungen erzwungen sowie mehr oder weniger adäquate Verhaltens-„Vorschriften" für Mensch-Technik-Interaktionen hervorgebracht werden.




22 „Ein soziotechnisches System ist [...] ein Handlungs- oder Arbeitssystem, in dem menschliche und sachtechnische Subsysteme eine integrale Einheit bilden" (Ropohl 1999, S. 142).
23 Hörning 1985, S. 199.





Kombiniert man nun die Aussagen zu einem erweiterten Sicherheits- und zu einem erweiterten Technikverständnis, dann ergibt sich die nachfolgende Zusammenstellung (siehe Abbildung 2).[24]

Abbildung 2: Technik- und Sicherheitsverständnisse[25]





TECHNIKVERSTÄNDNISSE		SICHERHEITSVERSTÄNDNISSE	KRITERIEN FÜR TECH-NIKSICHERHEIT
enges Technikver-ständnis	Technik als Real-technik/ technisches Sachsystem/ technisches Artefakt	Technik als Problemquelle	Funktionsfähigkeit der Sachtechnik
mittelweites (mittleres) Technikver-ständnis	Technik als Mensch-Maschine-System (MMS) bzw. Mensch-Ma-schine-Interaktion	Mensch als Problemquelle	Arbeitssicherheit
	Technik als soziotechnisches System	Interaktion zwischen sozialem und technischem System als Problemquelle	reibungslose Interakti-on zwischen sozialem und technischem System
	Technik als kulti-vierte Technik	dysfunktionale Beziehung zwischen verschiedenen Kolle-ktiven, die mit einer Technik umgehen, als Problemquelle	sicherheitskulturelle Aspekte in Unterneh-menskulturen
	Technik als Medium		
weites Technikver-ständnis	Technik als Hand-lungspraxis/ gelingende Regel-Reprodu-zierbarkeit		(reproduzierbare Regel-anwendung)

24 Vgl. Banse/Hauser 2008b; Banse/Hauser 2009.
25 Nach Banse/Hauser 2009.





3.3 „SICHERHEITSKULTUR" ALS LEITBEGRIFF EINER NOCH EINZULÖSENDEN FORSCHUNGSPROGRAMMATIK

Aus diesen Überlegungen wird deutlich, dass Technikerzeugung wie -nutzung in einer (auch) kulturell verfassten „Umwelt" erfolgen, die auch relevant für die Gewährleistung bzw. Realisierung von (Technik-)Sicherheit ist. Zu thematisieren ist damit das kulturelle Selbstverständnis einer Gesellschaft einschließlich ihres „Sicherheitsverständnisses" (Sicherheitsbedürfnis, Unsicherheitserfahrung, Gefahrenvorsorge, Kommunikation über mögliche Vor- und Nachteile bzw. „Gewinne" und „Verluste").[26] Damit wird zugleich die Grenze des je zeit- und kontextabhängigen akzeptablen bzw. akzeptierten Technik nutzenden Handelns (zum Beispiel hinsichtlich des Sicherungsaufwands, des Verhältnisses von Kosten und Nutzen oder der Einfachheit der Handhabung) festgelegt, deren Überschreitung zu individuellen wie institutionellen „Abwehrreaktionen" (Ablehnung, uneffektive Nutzung, Rückgriff auf konventionelle Lösungen und Ähnliches) führen kann. Über das individuelle Sicherheitsbedürfnis und -verlangen hinaus haben verschiedene soziale Gruppen einen je unterschiedlichen kollektiven Umgang mit Unbestimmtheiten, Gefahren und Risiken der Technik entwickelt. Eine Lösung der mit den individuellen und subjektiven Sicherheitsbedürfnissen verbundenen Probleme kann nur in der Entwicklung von angemessenen Sicherheitskulturen in dem unauflösbaren Spannungsfeld der Integrität von Individuum und Gesellschaft liegen.

Mit „Kultur" seien hier sowohl die Wertvorstellungen, Überzeugungen, Kognitionen und Normen, die von einer Gruppe von Menschen geteilt werden, als auch die Verhaltensweisen und Praktiken, die für eine Gruppe von Menschen üblich sind, erfasst: „Culture is generally understood to mean the assumptions and beliefs that are rooted in a social system. It is reflected in a system of values and norms, as well as in tangible characteristics and the models of behaviour of the system's members".[27]

Kulturelles in Form von (tradierten) Werten oder Normen beeinflusst menschliches Verhalten – auch im Umgang mit technischen Sachsystemen. Dieser Zusammenhang wird zwar oftmals konstatiert, belastbare empirische Belege gibt es jedoch kaum. Ein konzeptioneller Ansatz in dieser Richtung ist der der „Sicherheitskultur". Dieses Konzept ist noch nicht sehr alt und bislang wenig operationalisiert. International wurde es von der International Nuclear Safety Advisory Group (INSAG) im Jahre 1986 als Reaktion auf das Reaktorunglück in Tschernobyl in die Diskussion gebracht. Mit dem sogenannten Safety-Culture-Konzept hat sie darauf aufmerksam gemacht, dass neben den technischen Maßnahmen auch die soziokulturellen Aspekte von entscheidender Bedeutung sind. Im Jahre 1991 wurde durch eine internationale Beratergruppe der Begriff „Sicherheitskul-

---

[26] Vgl. dazu aus der „Risikoperspektive" Renn/Rohrmann 2000.
[27] Swiss Re 1998, S. 17.



tur" wie folgt definiert und in die Praxis eingeführt: ein „assembly of characteristics and attitudes in organisations and of individuals which establishes that, as an overriding priority, [nuclear] safety issues receive the attention warranted by their significance".[28] Erfasst, benannt und beschrieben werden somit *auch* kulturbedingte Elemente bzw. Komponenten, die für die Gewährleistung der Sicherheit technischer Handlungsvollzüge bedeutsam sind: „Beeinflußt werden die Charakteristika einer Sicherheitskultur durch technische, ökonomische und organisatorische Zwänge, repräsentiert werden sie durch sicherheitstechnische Vorrichtungen, Regelwerke, Vorschriften, Aufsichtsdienste und Praktiken einerseits sowie informelle Praktiken, individuelle und kollektive Sinnvorstellungen der Menschen andererseits. Sicherheitskulturen bieten für den einzelnen Menschen folglich einen Rahmen, der die Ordnung der menschlichen Wahrnehmung erst ermöglicht."[29]

Um diesen Kulturbegriff weiter differenzieren zu können, wird auf den Ansatz von Klaus P. Hansen zu Standardisierungen zurückgegriffen, die die Kultur von Gemeinschaften von Menschen (von Hansen „Kollektive" genannt) kennzeichnen.[30] Derartige Standardisierungen gibt es seinem Ansatz nach auf den Ebenen Kommunikation, Handeln/Verhalten, Denken und Fühlen/Empfinden. Die kulturellen Standardisierungen können hinsichtlich der Entstehung von Sicherheitskulturen auf der Ebene der Multikollektive (Mesoebene) durch folgende (exemplarische) Fragen präzisiert werden:[31]




1. *Kommunikation:* Wie wird über Techniksicherheit kommuniziert? Wie ist Kommunikation im Unternehmen organisiert? Welche konkreten Sprach- und Kommunikationspraxen haben sich herausgebildet?
2. *Handeln/Verhalten*: Welche sicherheitsrelevanten Handlungspraxen haben sich im Umgang mit Technik(en) bzw. technischen Systemen herausgebildet und wie sind diese institutionalisiert? Wie werden die Rahmenbedingungen des Primärkontextes (insbesondere Richtlinien, Verordnungen etc.) in das Handeln inkorporiert? Welche Verhaltensregeln haben sich „eingebürgert"? Welche Anerkennungsmechanismen für vorbildliches Verhalten bzw. welche Sanktionen bei Verstoß existieren?

---

[28] Zit. nach Swiss Re 1998, S. 18. – Rainer Pitschas hat, in einem gänzlich anderen Zusammenhang, das Konzept „Sicherheitskultur" eingeführt, „um kulturbedingte Verhaltensmerkmale zu beschreiben, die für die Gewährleistung der inneren Sicherheit in der EU [...] von Bedeutung sind. [...] Solchermaßen dimensionierte Sicherheitskultur prägt sich sowohl ‚intern' aus, nämlich als ein Set von Einstellungen und Werthaltungen des mit dem Schutz der inneren Sicherheit beauftragten Personals, ebenso aber auch ‚extern', nämlich in Gestalt von Einstellungen und Werthaltungen der Bevölkerung gegenüber Kriminalität, Recht und staatlichem Handeln sowie gegenüber dem Polizei- bzw. Verwaltungspersonal" (Pitschas 2000, S. 181).

[29] Hartmann 1995, S. 10.

[30] Vgl. näher Hansen 2003. Hansen differenziert Kulturen nach vier verschiedenen Kollektivebenen, wodurch eine analytische Trennung möglich wird (Segmentierung von Kulturen): Monokollektive (Kleinstgruppen wie beispielsweise Familien, bestehend aus Eltern und Kindern), Multikollektive (etwa ein Unternehmen), Dachkollektive (zum Beispiel ein Volk) und Globalkollektive (vgl. Hansen 2003, S. 194-234).

[31] Vgl. Banse/Hauser 2008a.





3. *Denken:* Welche Kompetenzen und welchen Informationsstand haben die Akteure? Welche Sensibilität und Akzeptanz haben sie? Welche impliziten Werte und Normen bestimmen als Annahmen und Deutungen (allgemein: „Bilder") das Denken (und damit auch das Handeln/Verhalten)?
4. *Fühlen/Empfinden:* Wie zufrieden sind die Individuen mit der Arbeitsumgebung? Welche Strukturen der Anerkennung und Motivation existieren? Wie sicher oder unsicher fühlen sich die Individuen? Wie wird mit „gefühlten" Unsicherheiten im Kollektiv umgegangen? Wie hoch ist das Vertrauen in die Technik, aber auch in die Institutionen?

In Bezug auf Techniksicherheit wurden Sicherheitskulturen bisher vor allem in sogenannten Hochrisiko-Technologiebereichen (Kernkraftwerke, Chemieunternehmen, Luftfahrt) als konzeptioneller Ansatz relevant,[32] aber auch im Bereich der IT-Branche oder der Logistik. Zunehmend finden sich Überlegungen zum integrierten betrieblichen Sicherheitsmanagement außerhalb dieses Bereiches. „Sicherheitskultur" wurde damit zum Schlüsselbegriff für das Sicherheitsverhalten aller Mitarbeiter in einem Unternehmen und in diesem Sinne Teil der Unternehmenskultur. Dabei wird Sicherheitskultur nicht nur intra-, sondern – vor allem als Folge von Globalisierungsprozessen – auch interkulturell relevant.



Deutlich wird, dass „Sicherheitskultur" sowohl eine mehr „theoretische" Ebene (vor allem in Form von Anweisungen, Regeln, Vorschriften, Statements, Codes usw.) als auch eine „praktische" Ebene (als gelebte und praktizierte Sicherheitskultur) besitzt. Oder anders ausgedrückt: Auf der praktischen Ebene umfasst Sicherheitskultur die sicherheitsbezogenen Einstellungen, Werte und grundlegenden Überzeugungen der Mitarbeiter bzw. Nutzer.

Mit Hans-Jürgen Weißbach sind Sicherheitskulturen in Unternehmen zunehmend heterogen, aber auch „hybrid". So gibt es zum Beispiel an Fertigungsstraßen oder selbst an einzelnen Anlagen eine große Pluralität jener Berufsgruppen, die für die Sicherheit einer Anlage zuständig sind. In einer Fertigungsstraße etwa arbeiten nicht nur Mechani-

32 Vgl. zum Beispiel KSA 2004.





ker und Maschinenbauer, sondern auch Hydrauliker, Elektriker, Elektroniker, Regeltechniker und Programmierer, die – vom Facharbeiter bis zum Ingenieur – auf verschiedenen Kompetenzniveaus arbeiten. Deshalb lässt sich das „Aufeinanderprallen" einer Vielzahl von Sicherheitsauffassungen sowie sicherheitsbezogener Normen und Werte konstatieren, ohne dass sich für diesen Vorgang eindeutige Hierarchien oder Übersetzungen finden lassen.[33] Das trifft auch auf andere Unternehmensbereiche zu.

Hervorzuheben ist, dass Kultur(en) stets implizite Werthaltungen einschließen, da diese einen großen Einfluss auf unterschiedliche Sicherheitskulturen haben. Damit sind „stillschweigend" vorausgesetzte Handlungs- und Verhaltens-„Regeln" gemeint, denen Menschen folgen, „ohne sie in ihrer ganzen Tragweite überblicken zu können".[34] Dazu schreibt Horst Hegmann: „Von den Vorgaben der eigenen Weltsicht können sich die in ihr Aufgewachsenen schon deshalb nicht ohne weiteres emanzipieren, weil ihnen Teile des so vermittelten Wissens dauerhaft unbewusst bleiben müssen".[35] Es gilt also, unreflektierte Denkgewohnheiten und Handlungsprogramme der Akteure zu identifizieren und ihre Wirkung bei der Analyse mit zu berücksichtigen. Dazu nochmals Hegmann: „Dass sich die impliziten Aspekte einer Kultur der bewussten Reflexion entziehen, ist für die Analyse [...] so lange relativ unschädlich, wie Akteure und Beobachter vor dem Hintergrund derselben Kultur agieren bzw. Handeln analysieren. [...] Anders ist es, wenn die Menschen jeweils unterschiedliche Kontexte im Hinterkopf haben. Nur wo der kulturelle Kontext der in Frage stehenden Regel für alle Beteiligten derselbe ist, kann durch ihn gekürzt werden".[36]




Für Sicherheitskulturen ist schließlich auch bedeutsam, dass nicht alle relevanten Akteure innerhalb einer Sprachgemeinschaft (etwa Konstrukteure und Nutzer) die gleichen impliziten Werthaltungen besitzen bzw. ihnen folgen müssen. Das kann schwerwiegende Folgen haben (zum Beispiel sprachliche Missverständnisse oder Übersetzungsfehler als Auslöser von Irrtümern mit Unfallfolgen). Deshalb sind diese impliziten Grundlagen möglichst weitgehend zu explizieren, um sie kommunizieren und in technische Regelwerke und Ähnliches transformieren zu können.

Im Kontext der Intrakulturalität von Sicherheitskultur werden unter anderem folgende Themen debattiert:

- Technikeinsatz, Arbeitsorganisation und Sicherheitskultur;
- Sicherheitskultur als Zusammenspiel von Mensch, Technik und Organisation;
- menschliche Fehlhandlungen und fehlerfreundliche Technik;
- Differenz zwischen verordneter, formaler und realisierter Sicherheit(skultur);
- Erfassung, Bewertung und Beförderung von Sicherheitskulturen.

---

33 Vgl. Weißbach 1993, S. 97f.
34 Hegmann 2004, S. 15.
35 Hegmann 2004, S. 16.
36 Hegmann 2004, S. 18 f.





Da die Entwicklung von technischen Sachsystemen unterschiedlichster Größenordnung eng in (technische) Kulturen eingebunden ist, ist davon auszugehen, dass die impliziten Werte und Normen, die sich unter anderem in Operationsroutinen „vergegenständlichen" und konstituierende Elemente von Sicherheitskulturen sind, nicht nur prägend auf das technische Handeln, sondern auch auf das technische Sachsystem selbst wirken. Daher kann der Import von Technik, die in anderen Technik- und Sicherheitskulturen konstruiert und gefertigt wurde, im aufnehmenden System und seinem kulturellen Kontext dazu führen, dass dessen Sicherheitskultur überfordert wird. Die Einführung kann im Ergebnis scheitern, weil das fremde Element nicht sicher eingefügt werden kann. Wenn eine „Normalisierung" im Umgang mit importierten Artefakten im Zielsystem nicht möglich ist, kann daraus eine dauerhafte Überforderung der Nutzer bzw. ein subprofessioneller Umgang mit dieser Technik resultieren. Bei dem Techniktransfer in andere Länder und damit andere Kulturen kommt hinzu, dass einerseits unterschiedliche Sicherheitskulturen (die der Ursprungs- und die der Zielregion) relevant werden, andererseits weitergehende, „höherstufige" sprachliche Verständigungsprozesse erforderlich sind.

Das Thema „Sicherheitskulturen" ist bisher nicht umfassend bearbeitet. Ansätze dazu finden sich derzeit vor allem im Bereich der Arbeitswissenschaften[37] sowie der Wirtschafts- und Sozialwissenschaften (Unternehmensmanagement). Darüber hinaus findet man Überlegungen seitens der Kulturwissenschaften, der Technikphilosophie, der Linguistik bzw. interkulturellen Kommunikation und des Wissensmanagements.[38]




Hinsichtlich des Vergleichs von Sicherheitskulturen in verschiedenen Unternehmen wie auch verschiedenen Ländern müssen, entsprechend dem oben Dargestellten, weitere konzeptionelle Zuschnitte gemacht werden. Es ist daher beim Vergleich von Sicherheitskultur(en) zunächst zwischen dem sogenannten Sekundärkontext auf der Makroebene und dem sogenannten Primärkontext auf der Mesoebene zu unterscheiden (vgl. Hansen 2003):

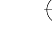
1. der Primärkontext[39] (bei intrakulturellen Vergleichen): sicherheitskulturrelevante Aspekte der Sprache, Geschichte und Institutionen des Unternehmens (hinsichtlich der Institutionen zum Beispiel Verordnungen, Regelungen, Richtlinien der Handhabung von Sicherheit im Umgang mit Technik(en) bzw. Techniksystemen wie zum Beispiel IuK-Technik: Security bzw. Safety Policies, Katastrophenerfahrungen, Gefahrenabwehrrituale etwa im Bergbau);

---

37 Vgl. zum Beispiel Grote/Künzler 2000; Künzler/Grote 1996.

38 Wegen der Vielfalt, aber auch wegen einer unbefriedigenden systematischen Erfassung wird hier auf die Angabe weiterführender Literatur bewusst verzichtet.

39 Der Primärkontext stellt nach Hansen die (immer besondere) historische Entwicklung sowie die damit verbundenen sprachlichen und institutionellen Entwicklungen der Technik dar. Der Primärkontext ist der speziell die Technik betreffende Teil des Sekundärkontextes bzw. in diesen eingebettet.



2. der Sekundärkontext[40] (bei interkulturellen Vergleichen): sicherheitskulturrelevante Aspekte der Sprache, Geschichte und Institutionen der Nationalkultur (hinsichtlich der Institutionen sind dies zum Beispiel Verfassungsgesetze, die über den „Wert" von Leben und Sicherheit im Allgemeinen verfügen, Ethikgremien, Urteile übergeordneter Gerichte wie des BVerG).

Beide Kontexte sind für die Konstitution von Sicherheitskulturen als Teil konkreter Unternehmenskulturen relevant.

Obwohl seit der „Geburt" des Konzepts der Sicherheitskultur Überlegungen in unterschiedlichen (wissenschaftsdisziplinären) Richtungen erfolgten, ist es jedoch immer noch eher ein programmatischer Ansatz geblieben. Die Gründe dafür sind vielfältig. Genannt seien lediglich drei.

- Erstens: Die vorliegenden Überlegungen haben zumeist entweder einen wirtschaftswissenschaftlichen Hintergrund und werden als Aspekt des Unternehmensmanagements (bzw. des Sicherheitsmanagements) eingeführt oder sie kommen aus dem Bereich der sogenannten Arbeitswissenschaften (wie Ergonomie, Arbeits- und Ingenieurpsychologie) und bleiben den jeweiligen disziplinären Paradigmen bzw. Konzeptualisierungen verhaftet.
- Zweitens: Häufig erfolgt keine Explizierung der zugrunde gelegten theoretischen Annahmen (insbesondere hinsichtlich Kultur- und Technikverständnis, Auffassung vom Menschen, Konzept der Mensch-Technik-Interaktion).
- Drittens: Eine Operationalisierung (und damit auch Vergleichbarkeit) von Sicherheitskulturen ist derzeit schlecht durchführbar, da (inter- wie intrakulturelle) Indikatoren bislang kaum entwickelt wurden.

3.4 LITERATUR

Bachmann 1991
Bachmann, C.: Sicherheit. Ein Urbedürfnis als Herausforderung für die Technik, Basel, Boston, Berlin: Birkhäuser Verlag, 1991.

Banse 1996
Banse, G. (Hrsg.): Risikoforschung zwischen Disziplinarität und Interdisziplinarität. Von der Illusion der Sicherheit zum Umgang mit Unsicherheit, Berlin: edition sigma, 1996.

[40] Nach Hansen bezieht sich der Sekundärkontext mit der Berücksichtigung der allgemeinen geschichtlichen, sprachlichen und institutionellen Entwicklungen und Strömungen der Nationalkultur, in denen konkrete Technik entwickelt, eingeführt und genutzt wird, auf den weiteren Referenzrahmen, in dem dann der Primärkontext betrachtet wird.







Banse 2002a
Banse, G.: „Johann Beckmann und die Folgen. Allgemeine Technologie in Vergangenheit und Gegenwart." In: Banse, G./Reher, E.-O. (Hrsg.): Allgemeine Technologie – Vergangenheit, Gegenwart, Zukunft, Berlin: trafo verlag, 2002, S. 17-46.

Banse 2002b
Banse, G.: „Über den Umgang mit Ungewissheit." In: Banse, G./Kiepas, A. (Hrsg.): Rationalität heute. Vorstellungen, Wandlungen, Herausforderungen, Münster u. a.: LIT-Verlag, 2002, S. 211-234.

Banse/Friedrich 1996
Banse, G./Friedrich, K.: „Technische Welterzeugung – Philosophische Aspekte." In: Hubig, C./Poser, H. (Hrsg.): Cognitio humana – Dynamik des Wissens und der Werte, (Workshop-Beiträge. XVII. Deutscher Kongress für Philosophie, Bd. 1), Leipzig: Universität, 1996, S. 334-341.

Banse/Hauser 2008a
Banse, G./Hauser, R.: „Technik und Kultur. Das Beispiel Sicherheit und Sicherheitskulturen." In: Rösch, O. (Hrsg.): Technik und Kultur, Berlin: Verlag News & Media / Marcus v. Amsberg, 2008, S. 51-83.



Banse/Hauser 2008b
Banse, G./Hauser, R.: „Technik als (Intra- und Inter-)Kulturelles. Exemplarisches." In: Gronau, N./Eversheim, W. (Hrsg.): Umgang mit Wissen im interkulturellen Vergleich. Beiträge aus Forschung und Unternehmenspraxis, Stuttgart: Fraunhofer IRB Verlag, 2008 (acatech diskutiert), S. 49-77.

Banse/Hauser 2009
Banse, G./Hauser, R.: „Technik und Kultur – ein Überblick." In: Banse, G./Grunwald, A. (Hrsg.): Technik und Kultur. Bedingungs- und Beeinflussungsverhältnisse, Karlsruhe: Universitätsverlag Karlsruhe, 2009 (im Erscheinen).

Bonß 1997
Bonß, W.: „Die gesellschaftliche Konstruktion von Sicherheit." In: Lippert, E./Prüfert, A./ Wachtler, G. (Hrsg.): Sicherheit in der unsicheren Gesellschaft, Opladen: Westdeutscher Verlag, 1997, S. 21-41.





Büttner/Fahlbruch/Wilpert 1999
Büttner, T./Fahlbruch, B./Wilpert, B.: Sicherheitskultur. Konzepte und Analysenmethoden, Heidelberg: Asanger Verlag, 1999.

Dörner 1989
Dörner, D.: Die Logik des Mißlingens. Strategisches Denken in komplexen Situationen, Reinbek bei Hamburg: Rowohlt Verlag, 1989.

Drews/Wacke/Vogel 1986
Drews, B./Wacke, G./Vogel, K.: Gefahrenabwehr II. Allgemeines Polizeirecht (Ordnungsrecht) des Bundes und der Länder, 9. Aufl. Köln: Heymanns Verlag, 1986.

Frederichs/Bechmann 1997
Frederichs, G./Bechmann, G.: „Zum Verhältnis von Natur- und Sozialwissenschaften in der Klimawirkungsforschung." In: Kopfmüller, J./Coenen, R. (Hrsg.): Risiko Klima. Der Treibhauseffekt als Herausforderung für Wissenschaft und Politik, Frankfurt/Main, New York: Campus Verlag, 1997, S. 75-118.



Gethmann/Kloepfer 1993
Gethmann, C. F./Kloepfer, M.: Handeln unter Risiko im Umweltstaat, Berlin u. a.: Springer-Verlag, 1993.

Grote/Künzler 2000
Grote, G./Künzler, C.: "Diagnosis of Safety Culture in Safety Management Audits." In: Safety Science 34 (2000), S. 131-150.

Grunwald 1997
Grunwald, A.: „Kulturalistische Planungstheorie." In: Hartmann, D./Janich, P. (Hrsg.): Methodischer Kulturalismus. Zwischen Naturalismus und Postmoderne, Frankfurt/Main: Suhrkamp Verlag, 1997, S. 315-345.

Grunwald 2009
Grunwald, A.: „Technisierung als Bedingung und Gefährdung von Kultur. Eine dialektische Betrachtung." In: Banse, G./Grunwald, A. (Hrsg.): Technik und Kultur. Bedingungs- und Beeinflussungsverhältnisse, Karlsruhe: Universitätsverlag Karlsruhe, 2009 (im Erscheinen).





Guggenberger 1987
Guggenberger, B.: Das Menschenrecht auf Irrtum. Anleitung zur Unvollkommenheit, München: Carl Hanser Verlag, 1987.

Hansen 2003
Hansen, K. P.: Kultur und Kulturwissenschaft, 2. Aufl. Tübingen, Basel: Francke-Verlag, 2003.

Hartmann 1995
Hartmann, A.: „'Ganzheitliche IT-Sicherheit': Ein neues Konzept als Antwort auf ethische und soziale Fragen im Zuge der Internationalisierung von IT-Sicherheit." In: BSI – Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Fachvorträge 4. Deutscher IT-Sicherheitskongreß 1995, (Sektion 7, BSI 7165), S. 1-13.

Hegmann 2004
Hegmann, H.: „Implizites Wissen und die Grenzen mikroökonomischer Institutionenanalyse." In: Blümle, G./Goldschmidt, N./Klump, R./Schauenberg, B./von Senger, H. (Hrsg.): Perspektiven einer kulturellen Ökonomik, Münster: LIT-Verlag 2004, S. 11-28.




Hörning 1985
Hörning, K- H.: „Technik und Symbol. Ein Beitrag zur Soziologie alltäglichen Technikumgangs." In: Soziale Welt 36 (1985), S. 185-207.

Hofmann 2008
Hofmann, M-: Lernen aus Katastrophen. Nach den Unfällen von Harrisburg, Seveso und Sandoz, Berlin: edition sigma, 2008.

Holz 1992
Holz, H- H-: Philosophie der zersplitterten Welt. Reflexionen über Walter Benjamin, Köln: Pahl-Rugenstein, 1992.

Kaufmann 1973
Kaufmann, F–X-: Sicherheit als soziologisches und sozialpolitisches Problem. Untersuchungen zu einer Wertidee hochdifferenzierter Gesellschaften, 2. Aufl. Stuttgart: Enke Verlag, 1973.



Künzler/Grote 1996
Künzler, C./Grote, G.: „SAM – Ein Leitfaden zur Bewertung von Sicherheitskultur in Unternehmen." In: Rüttinger B./Nold, H./Ludborzs, B. (Hrsg.): Psychologie der Arbeitssicherheit. 8. Workshop 1995, Heidelberg: Asanger Verlag, 1996, S. 78-93.

KSA 2004
Eidgenössische Kommission für die Sicherheit von Kernanlagen (KSA): Sicherheitskultur in einer Kernanlage. Erfassung, Bewertung, Förderung, (KSA-Report, Nr. 04-01), Januar 2004.

Lippert/Prüfert/Wachtler 1997
Lippert, E./Prüfert, A./Wachtler, G.: „Einleitung." In: Lippert, E./Prüfert, A./Wachtler, G. (Hrsg.): Sicherheit in der unsicheren Gesellschaft, Opladen: Westdeutscher Verlag, 1997, S. 7-20.

Perrow 1989
Perrow, C.: Normale Katastrophen. Die unvermeidbaren Risiken der Großtechnik, Frankfurt/Main, New York: Campus Verlag, 1989.



Pitschas 2000
Pitschas, R.: „Interkulturelle Verwaltungskooperation in der Europäischen Union. Zur kulturellen Kontextsteuerung der polizeilichen und justiziellen Zusammenarbeit im Rahmen des Europäischen Sicherheitsrechts." In: Deutsche Hochschule für Verwaltungswissenschaften Speyer (Hrsg.): Speyer-Jahrbuch 1: „Speyerer Initiativen für die Praxis", Speyer, 2000, S. 175-195.

Renn/Rohrmann 2000
Renn, O./Rohrmann, B. (Hrsg.): Cross-cultural Risk Perception. A Survey of Empirical Studies, Dordrecht, Boston, London: Kluwer Academic Publishers, 2000.

Reuter/Wehner 1996
Reuter, H./Wehner, T.: „Eine ganzheitspsychologische Betrachtung der Sicherheit im Umgang mit Industrierobotern." In: Banse, G. (Hrsg.): Risikoforschung zwischen Disziplinarität und Interdisziplinarität. Von der Illusion der Sicherheit zum Umgang mit Unsicherheit, Berlin: edition sigma, 1996, S. 93-103.





Robbers 1987
Robbers, G.: Sicherheit als Menschenrecht. Aspekte der Geschichte, Begründung und Wirkung einer Grundrechtsfunktion, Baden-Baden: Nomos Verlagsgesellschaft, 1987.

Ropohl 1999
Ropohl, G.: Allgemeine Technologie. Eine Systemtheorie der Technik, 2. Aufl. München, Wien: Carl Hanser Verlag, 1999.

Swiss Re 1998
Swiss Re – Swiss Reinsurance Company: Safety Culture – a Reflection of Risk Awareness, Zürich (Swiss Re), 1998.

VDI 1991
Verein Deutscher Ingenieure (VDI): Technikbewertung – Begriffe und Grundlagen. VDI-Richtlinie 3780, Düsseldorf (VDI), 1991.

Wehner 1992
Wehner, T. (Hrsg.): Sicherheit als Fehlerfreundlichkeit. Arbeits- und sozialpsychologische Befunde für eine kritische Technikbewertung, Opladen: Westdeutscher Verlag, 1992.




Weißbach 1993
Weißbach, H.-J.: „Kommunikative und kulturelle Formen der Risikobewältigung in der informatisierten Produktion." In: Weißbach, H.-J./Poy, A. (Hrsg.): Risiken informatisierter Produktion. Theoretische und empirische Ansätze – Strategien zur Risikobewältigung, Opladen: Westdeutscher Verlag, 1993, S. 69-102.

Wildavsky 1984
Wildavsky, A.: „Die Suche nach einer fehlerlosen Risikominimierungsstrategie." In: Lange, S.: Ermittlung und Bewertung industrieller Risiken, Berlin u. a.: Springer-Verlag, 1984, S. 244-234.





4 SICHERHEITSMODELLE UND KOMMUNIKATIONS-RISIKO

ANNELY ROTHKEGEL

4.1 FRAGESTELLUNG

Die Kommunikation von „Sicherheit" verläuft vor dem Hintergrund der zugrunde gelegten Sicherheitsmodelle, die jeweils durch bestimmte Merkmale gekennzeichnet sind. Die Frage stellt sich, ob es typische Kommunikationsmuster gibt, die den Rahmen für bestimmte Konfigurationen solcher Merkmale determinieren. Umgekehrt kann gefragt werden, welche Sicherheitsmodelle für welche Kommunikationszwecke bzw. Kommunikationssituationen relevant sind. Dabei wäre von Interesse, welche Merkmalkonfigurationen in und durch Kommunikation vorausgesetzt, entwickelt und vermittelt werden. Die Voraussetzungen beziehen sich auf das Hintergrundwissen der an der Kommunikation Beteiligten. Mit „Entwicklung" ist gemeint, dass die Modelle im dialogischen Austausch bzw. im Diskurs weiter elaboriert und spezifiziert werden. Die Vermittlung schließlich bezieht die Transformationen ein, die die ursprünglich in die Kommunikation eingebrachten Sicherheitsmodelle durch Anpassung erfahren. Mit Blick auf die fachexterne Kommunikation ergeben sich Probleme aus der Tatsache, dass Begriffssysteme eine dynamische Angelegenheit sind. Ein Großteil sogenannter Sachdiskussionen sind Diskussionen um begriffliche Abgrenzung und Zurechtrückung. In der internationalen Kommunikation kommen kulturell bestimmte Unterschiede zu den sprachlichen hinzu. Das Kommunikationsrisiko ist weiterhin erhöht. Entsprechend bemüht man sich in internationalen Normungsausschüssen um Harmonisierung, das heißt um Festlegungen für den Gebrauch, die aus dem Angebot möglicher Definitionen ausgefiltert werden.[1]

[1] Die Unsicherheit im Umgang mit Begriffen gehört zu den Themen der Fachkommunikation (Hoffmann et al. 1998) und Terminologieforschung (Budin 1996, Gerzymisch-Arbogast 1996) bzw. ist Gegenstand der Terminologiearbeit in der Praxis (Arntz/Picht/Mayer 2004). Es sind drei Aspekte, die im Vordergrund stehen:

1. die Abgrenzung der Begriffe/Fachbegriffe untereinander,
2. die Zuordnung von Begriff (mentalem Konzept) und Benennung (einzelsprachlichem Ausdruck),
3. die Kontextualisierung (Abhängigkeit der Bedeutung vom Verwendungskontext).





In diesem Beitrag werden der begriffliche Hintergrund einiger unterschiedlicher Sicherheitsmodelle skizziert und einige Gründe für Kommunikationsrisiken demonstriert, die in der Experten-Nichtexperten-Kommunikation zum Tragen kommen. Mit der linguistischen Text- und Dialoganalyse wird eine Methodik angedeutet, die für die empirisch fundierte Suche nach typischen Mustern der Sicherheitskommunikation geeignet erscheint.[2]

4.2 RISIKO-MODELL UND EREIGNISSTRUKTUR

Modelle (im Sinne von mentalen Modellen)[3] vermitteln eine Sicht auf die „Welt", die die Komplexität reduziert und dabei einen bestimmten Gesichtspunkt hervorhebt, unter dem die betrachteten Einheiten und Relationen einen Zusammenhang bilden. Ein mögliches Sicherheitsmodell wird in Klassifikationssystemen und Ontologien abgebildet. Die Einheiten sind die Begriffe, die einen Sach- oder Fachbereich gliedern. Linguistisch gesprochen geben sie den Referenzbereich (Gegenstandsbereich) an, der für die Kommunikation im Fach und darüber hinaus relevant ist. Systematisch strukturiert in Hierarchien oder semantischen Netzen bilden sie Ontologien, also „Ordnungen von Welt". Dabei wird die jeweilige „Welt" begrenzt auf eine Domäne (zum Beispiel den Wissensbereich einer Disziplin, Teildisziplin oder Branche). Diese Gliederung ist abhängig vom jeweiligen Wissens- und Diskussionsstand im Fach. Ihm entspricht die Zuordnung der Begriffsbedeutung zu den spezifischen Merkmalen. Diese ist mitbestimmt durch die Position des einzelnen Begriffs in Relation zu den anderen Begriffen innerhalb der Gesamtstruktur (zum Beispiel innerhalb eines Netzwerks). Im Folgenden steht ein Modell von Sicherheit im Fokus, das geprägt ist durch die enge Verknüpfung der beiden theoretischen Begriffe „Sicherheit" und „Risiko".

Die Risikoforschung der neunziger Jahre[4] hat eine Reihe von Systematiken entwickelt, die auch noch heute im Umfeld des Begriffs „Sicherheit" eine Rolle spielen. Für die nachfolgenden Überlegungen sind drei Aspekte zum Begriff „Risiko" relevant:

- die Unterscheidung der disziplinären Betrachtungsweisen:
  - Naturwissenschaft/Technik: Kontrollierbarkeit versus Unkontrollierbarkeit
  - Ökonomie: Gewinn versus Verlust
  - Sozialwissenschaften: Akteure und Betroffene
- die Definition als Relation zwischen Eintrittswahrscheinlichkeit und Schadensschwere

[2] Als Querschnittsdisziplin liefert die Linguistik Instrumente zur Analyse und Deskription von Phänomenen wie Begriffsordnungen und Terminologie sowie zu Verständlichkeit und Verstehen von Texten und Dialogen. Die Semantik beschäftigt sich mit der Erfassung und systematischen Ordnung der Bedeutungsbildung (Löbner 2003, in Bezug auf die Organisation von Wissen und Schemata Konerding 1993 sowie Ziem 2008), die Pragmatik mit dem Sprachgebrauch und kommunikativen Handeln im Kontext (Heinemann/Heinemann 2002, Schröder 2003, Ehlich 2007).

[3] Johnson-Laird 1983; Kutzner 1991.

[4] Vgl. Krüger/Ruß-Mohl (1991); Überblick in Banse/Bechmann 1998.







- die Perspektive auf die Dreiteilung von Schadensereignissen mit
  - Vor-Ereignis (Pre-Event)
  - Während-Ereignis (In-Event)
  - Nach-Ereignis (Post-Event)

In diesem Zusammenhang findet sich der Begriff „Sicherheit“ in den Aspekten der Kontrollierbarkeit wieder sowie in den Maßnahmen der Prävention, also zum Vor-Ereignis. Zur Prävention gehören unter anderem Risikowahrnehmung, Risikoidentifikation, Risikoanalyse, Risikoabschätzung, Risikoverminderung bzw. Risikokompensation. Die Risikoverminderung bezieht sich wiederum sowohl auf die Verringerung der Eintrittswahrscheinlichkeit (Häufigkeit von Unfällen) als auch der zu erwartenden Schadensschwere. Diese Merkmale der Risikodefinition unterliegen wiederum einem gewissen Unsicherheitsfaktor (Uncertainty). Innerhalb dieses Kontextes wird Sicherheit zur Reduktion von Risiko, das berechnet wird.



4.3 MASSNAHMEN-MODELL UND SCHLÜSSELBEGRIFFE („SAFETY“ UND „SECURITY“)

In den Ontologien werden die Ordnungen der Begriffe untereinander betrachtet. Dies ist eine semantische Sichtweise. In einer pragmatischen Sichtweise schaut man auf die Bedeutungsbildung, die durch den Kontext der Kommunikation bestimmt wird. Wissen wird zu Wissensgebrauch mit Themen und Zielen.[5] Mit dem Thema kommt eine Fragestellung in den Blick, auf die in einem Text oder Dialog bzw. einem daraus entstehenden Diskurs Antworten entwickelt werden. Diese Antworten wiederum zielen auf Veränderungen in der Realität. Bleiben wir zunächst bei den thematischen Aspekten und wie sie sich begrifflich auswirken. Mit der jeweiligen Fragestellung geht es um Selektion und Fokussierung von Wissensbeständen, die in einen neuen, thematischen Zusammenhang gebracht werden. Begriffe, die diesen Zusammenhang kennzeichnen, heißen „Schlüsselbegriffe“ (oder „Schlüsselkonzepte“, „Schlüsselwörter“, „Key Words“).[6] Ein Beispiel hierfür sind die englischen Ausdrücke „Safety“ und „Security“, für die es im Deutschen keine entsprechende Lexikalisierung gibt. Man arbeitet mit Äquivalenten wie „Betriebssicherheit“ oder „Produktsicherheit“ im Sinne von „Zuverlässigkeit“ für „Safety“ und Komposita, die die Bedeutungskomponente „Schutz vor“ enthalten, für „Security“ („vor wem oder was wird geschützt“, zum Beispiel „Diebstahlschutz“, „Virenschutz“). Zum Vergleich: Die Komposition „Kinderschutz“ enthält dagegen die Komponente „Schutz

5 Rothkegel 2009.

6 Villiger 2008; zu den Bedeutungswandlungen von Schlüsselbegriffen vgl. Liebert 2003 und Sommerfeldt 2008.







von“, hat also eine andere Bedeutung („wer oder was wird geschützt“), ähnlich wie Datenschutz (ein Ausdruck, der aber auch mit „Datensicherheit“ zusammengebracht wird). Als Schlüsselbegriffe sorgen „Safety“ und „Security“ für eine Unterscheidung, die es, wenn auch nicht lexikalisiert, auch im deutschen Sprachgebrauch gibt. Dabei bildet das Merkmal der Gefahr durch eine intendierte Attacke von außen (Security) gegenüber einem möglichen Geschehen (Safety) ein eher schwaches Merkmal, wenn es grundsätzlich um Sicherheit geht. Was damit gemeint ist, wird dadurch nicht geklärt. Als Nächstes ist die Frage zu stellen, ob ein Sicherheitsmodell aus der Praxis Aufschluss geben kann, in dem die Maßnahmen im Vordergrund stehen.

Dazu sei die existierende Sicherheitskommunikation ausgewählt, wie sie in der Technischen Dokumentation zum Standard gehört. Die Dokumentationspflicht bezieht sich auf folgende Anforderungen:

- Grad der Gefahr: Aufmerksamkeit soll erzeugt werden;
- Art und Quelle der Gefahr: Die Aufmerksamkeit soll auf die Gefahrenquelle gelenkt werden;
- mögliche Folgen: Es soll die Motivation zum Handeln dagegen geschaffen werden;
- Maßnahmen zur Gefahrenabwehr: Das für den Fall geeignete Handeln soll deutlich gemacht werden.



In der Praxis gibt es keinen einheitlichen Gebrauch bei der Kombination der einzelnen Komponenten. Dies mag unter anderem in der generellen Unsicherheit darüber begründet sein, welches Modell von Sicherheit als relevant für die Branche oder das betreffende Produkt einzustufen ist. Generell gilt aber, dass der Grad der Gefahr weiterhin in einer Skala abgestuft wird. Zu den unterscheidenden Merkmalen gehören einerseits das Schadensziel (Person, Sache, Infrastruktur, Umwelt), andererseits die Schadensschwere (hoch, mittel, leicht, geringfügig). Die in den Normen angezeigte Forderung zur Erzeugung der Aufmerksamkeit wird durch die Verwendung von sogenannten Signalwörtern (GEFAHR/DANGER, WARNUNG/WARNING, ACHTUNG oder VORSICHT/CAUTION), teilweise gekoppelt mit Piktogrammen, ausgeführt. Darüber hinaus kommen noch HINWEISE vor, die verwirrenderweise auch außerhalb der Sicherheitsdokumentation verwendet werden (verschiedentlich auch ACHTUNG):

- GEFAHR (DANGER):
  - unmittelbar drohende Gefahr mit Tod oder schwersten Verletzungen als Folge;
- WARNUNG (WARNING):
  - möglicherweise gefährliche Situation mit Tod oder schwersten Verletzungen als Folge;





- ACHTUNG oder VORSICHT (CAUTION):
  - gefährliche Situation mit geringfügigen Verletzungen oder möglichen Sachschäden
- HINWEIS:
  - möglicherweise schädliche Situation mit Produkt- oder Umgebungsschäden als Folge.

Interessant ist die Unterscheidung von GEFAHR und WARNUNG, wobei die Risikodefinition (siehe oben) implizit eine Rolle spielt. Die Schadensschwere ist in beiden Fällen gleich, doch nicht die Eintrittswahrscheinlichkeit, verbalisiert als „unmittelbar drohende Gefahr" bzw. „möglicherweise gefährliche Situation". Denkbar sind Situationen, wenn an laufenden Maschinen oder im Bereich von Robotern gearbeitet wird (GEFAHR), während sich die WARNUNG auf Situationen bezieht, die erst unter bestimmten Bedingungen zur Gefahr werden (zum Beispiel auf eine Explosionsgefahr). Die Merkmale der Risikodefinition tragen also zur Unterscheidung von Gefahrensituationen bei. Diese Unterscheidung ist wichtig für die Thematisierung der Schutzmaßnahmen: „Welche Maßnahmen sind geeignet für welche Gefahrensituationen?"





Kommen wir nun zu diesen Maßnahmen der Abwehr. Als „geeignetes Handeln" sollen sie deutlich gemacht werden und „die Motivation zum Handeln" soll erzeugt werden. Letzteres soll durch die Beschreibung der Folgen geschehen. Dies kann in den Produktinformationen sehr allgemein und unspezifisch formuliert sein, zum Beispiel:

- Maßnahme: „Halten Sie sich an den bestimmungsgemäßen Gebrauch";
- Folge: „andernfalls kann es zu Gefahren für Gesundheit und Leben kommen".

In der folgenden, spezifischen Formulierung müssen dagegen die Maßnahme („Anschlüsse richtig anbringen") sowie der Aufmerksamkeitsgrad („es ist wichtig, dass die Anschlüsse richtig sind") geschlussfolgert werden:

- Gefahrenquelle: „Falsche Anschlüsse";
- Folge: „können zur Zerstörung von elektrischen Bauteilen führen".

Welches Sicherheitsmodell liegt diesem skizzierten Kommunikationstyp zugrunde? Zunächst ist die semantische Ursache-Folgen-Relation zu erkennen, die typisch für die Darstellung naturwissenschaftlich-technischer Ereignisse ist. Die Gefahrenquelle als Ursache und die möglichen Folgen werden ergänzt durch die Maßnahmen der Gefahrenabwehr, das heißt die Ursache-Folgen-Kette soll durch entsprechende Vorgänge oder Handlungen unterbrochen werden. Als Effekt davon werden Personen oder Objekte geschützt, das heißt Sicherheit wird hergestellt. In diesem Modell gilt „Sicherheit" als





Maßnahmen im Umgang mit den Gefahrenquellen einerseits („aktive Sicherheit") und den Folgen andererseits („passive Sicherheit"). Auf diesen Punkt ist im übernächsten Abschnitt zurückzukommen. An dieser Stelle kann aber gesagt werden, dass eine Unterscheidung von „Safety" und „Security" in dem skizzierten Sicherheitsmodell nicht relevant ist. Dies ist anders, wenn wir die Nutzungsszenarios einbeziehen.

4.4 NUTZUNGSSZENARIOS UND DIE AKTEURE

Es ist zwischen „Anwendung (Applikation) von Technik" und „Techniknutzung" zu unterscheiden. Die „Anwendung" bezieht sich auf die Ausführung der Funktionen bzw. Funktionalitäten. So wird von einem Auto erwartet, dass es störungsfrei fahren und halten kann, und von einer Software, dass eine Kalkulation stimmt oder eine Datei tatsächlich kopiert ist. In der Sicht auf die „Nutzung" kommen weitere Komponenten in den Blick: Akteure und Umfeld, in dem das System in erweiterte Einsatzmöglichkeiten einbezogen wird. Als Nutzer und Nutzerinnen gehen die Akteure (hier nicht als Betreiber gemeint) unmittelbar mit den Gefahrenquellen um. Im unmittelbaren Kontakt mit dem technischen System sind sie selbst an der Ausführung der Schutzmaßnahmen beteiligt. Aber sie bestimmen auch selbst die Aufgaben oder Zwecke, deretwegen, wann und in welchem Kontext sie das Gerät einsetzen. Und damit kommen weitere Komponenten des jeweiligen Kontextes hinzu. Die Relation zwischen zwei Faktoren (Gefahrenquelle und Folgen) im oben skizzierten Sicherheitsmodell wird hier ersetzt durch ein Trio: „System", „Akteur", „Umfeld" (vgl. das Beispiel Fahrzeug, Fahrer/Fahrerin, Fahrbahn). Dass es drei Faktoren sind, ist noch nicht so entscheidend. Entscheidend ist, welche Rollen sie in diesem Zusammenspiel übernehmen.[7]

Gehen wir davon aus, dass der Akteur die Rolle des verantwortlich Handelnden hat, so kommt damit automatisch der Aspekt der Intention hinzu. Technische Maßnahmen, die die Compliance des Akteurs und dessen „richtige" Aktivitäten voraussetzen, würden damit in den Safety-Bereich gehören. Technische Maßnahmen, die nicht davon ausgehen, sondern eine Schadensabsicht antizipieren, würden in den Security-Bereich fallen (Missbrauch, Attacke). Doch wie stellt sich dabei der Bezug zu Gefahrenquelle und Folgen dar? Metallteile auf der Fahrbahn bilden eine Gefahrenquelle unabhängig davon, wie sie dorthin gekommen sind. Und, um das beliebte Gedankenspiel zu erwähnen: Der Absturz eines Flugzeugs hat die gleichen Folgen unabhängig davon, ob der Absturz ein Unfall oder eine Attacke ist. Im Hinblick auf die Art der technischen Maßnahmen hat dies keine Konsequenz (bei den juristischen und sonstigen Maßnahmen sind die Unterschiede natürlich wichtig). Zu überlegen wäre allerdings, ob Maßnahmen technischer Art überhaupt zu treffen sind. Dies mag wieder von der spezifischen Risikosituation einschließlich des beteiligten Produkts abhängen. Was aber dennoch den Security-Be-

[7] Denkbar ist, dass das Trio wieder zum Duo schrumpft, wenn der Akteur zusammen mit dem Umfeld zu den Gefahrenquellen gezählt wird (vgl. „Mensch als Risikofaktor"), dessen Einfluss durch technische Lösungen so weit wie möglich eingeschränkt werden sollte, zum Beispiel durch Assistenzsysteme. Ein anderer Ansatz besteht in der Gleichsetzung von System und Akteur, der dabei die Rolle des Bedieners hat.





reich auch unter technischen Gesichtspunkten interessant macht, ist die hervorgehobene Rolle des Schadensziels. Hier stehen Anfälligkeit und Verletzlichkeit als Merkmale im Vordergrund. „Sicherheit" bezieht sich in diesem Fall auf ein Modell, in dem solche Maßnahmen relevant sind, die insbesondere dem Schutz des Schadensziels hinsichtlich seiner Anfälligkeiten und Verletzlichkeiten gelten.

Gefahrenquelle und Schadensziel sind komplementäre Dimensionen (ein Grenzfall liegt vor, wenn beide zusammen fallen). Beziehen wir diesen Punkt auf die Relationen zwischen den Faktoren System, Akteur und Umfeld, so ist festzustellen, dass jeder Faktor sowohl in der einen wie in der anderen Dimension gesehen werden kann. Das System kann Gefahrenquelle sein und einen Schaden für Akteur und/oder Umfeld verursachen. Am Beispiel Auto: CO2-Ausstoß ist gesundheitsgefährdend für den Akteur und schädlich für die Umwelt. Der Akteur kann Gefahrenquelle sein für das System (Fehlgebrauch oder Missbrauch) und es beschädigen oder zerstören, was eine Folge für das Umfeld haben kann (Störung der Infrastruktur). Oder er wirkt auf das Umfeld ein (herbeigeführter Stromausfall), was eine Schadensfolge für das System bedeuten kann (Ausfall von Computern). Das Umfeld kann Gefahrenquelle sein (Unwetter, Glatteis), damit das System schädigen (Einfrieren von Mitteln, die zum Fahren benötigt werden), was zur Folge hat, dass auch der Akteur durch den Ausfall geschädigt wird.



Die Dynamik in der gerichteten Relation von Gefahrenquelle und Schadensziel kann verwendet werden, um hier die Begriffe „Safety" und „Security" einzuordnen oder zu einer dritten Einteilung zu kommen. So käme es auf den Impuls an, der als Gefahrenquelle die Dynamik in Gang setzt und sich auf ein spezifisches Schadensziel richtet. Stellen wir diese Relation in den Vordergrund, kann sie als Kriterium für die Festlegung der Gegenmaßnahmen gelten. Richtet sie sich auf die Gefahrenquelle, geht es um Safety-Maßnahmen (Abwehr von Gefahr). Bezieht sie sich auf das Schadensziel und seine anfälligen bzw. verletzlichen Komponenten, haben wir es mit Security-Maßnahmen zu tun (Schutzmaßnahmen). Das für den Schutz nicht-taugliche Merkmal der Intention (vorhanden oder nicht vorhanden) hinter der Einwirkung würde damit überflüssig.

4.5 MODELLE UND BENENNUNGSSTRATEGIEN

Den Begriffen zugeordnet sind die einzelsprachlichen Ausdrücke (Benennungen). Die Trennung von Begriff und Benennung ist zentral in der Terminologielehre.[8] Ein Problem ergibt sich, weil auch Begriffe sprachlich ausgedrückt werden. Verschiedentlich hilft man sich hier mit unterschiedlicher Schreibweise. So könnte man den Begriff SICHERHEIT vom Wort „Sicherheit" unterscheiden. Im Hinblick auf die Verständigung geht es um Begriffe; den Zugang zu ihnen ermöglichen aber die Benennungen.[9]

8 Göpferich/Schmitt 1996; Hennig/Tjarks-Sobhani 2008.
9 King 2008.





Kommunikationsprobleme können entstehen, wenn gleiche Benennungen für unterschiedliche Begriffe (Polysemie) oder unterschiedliche Benennungen für den gleichen Begriff verwendet werden (Synonymie). Kommen wir hier auf das oben bereits eingeführte Beispiel der „aktiven" und „passiven Sicherheit" im Bereich Automobil zurück.[10] Die Benennung „aktive Sicherheit" bezieht sich auf Maßnahmen der Prävention (Vor-Ereignis), das heißt das Risiko bzw. die Gefahr eines Unfalls soll vermindert werden (zum Beispiel durch die Funktionsweise der Bremsen). Die Benennung „passive Sicherheit" bezieht sich dagegen auf die Situation bei einem Unfall (Während-Ereignis). Es geht um Schutzmaßnahmen, die sich auf Personen als Schadensziel richten und die Verminderung der Unfallfolgen bezwecken (zum Beispiel durch Airbags). Die Benennung folgt einem Modell von Schadensabwehr und Schadensbegrenzung im Rahmen der Einteilung der Schadensereignisse. „Aktive" und „passive Sicherheit" in Bezug auf Fahrassistenzsysteme unterscheiden sich dagegen in anderer Weise. Die Benennung „aktive Sicherheit" steht hier für die Eigenschaft, dass das System ins Fahrgeschehen eingreift (zum Beispiel Spurhalteassistent). Die Benennung „passive Sicherheit" verweist auf die Eigenschaft, dass das System eine (visuelle oder akustische) Warnung abgibt. Für die Benennung steht eine Art Partnermodell im Hintergrund. „Aktiv" signalisiert die Rolle des die Aktionen initiierenden Partners, während „passiv" die Rolle des unterstützenden, Feedback gebenden Partners kennzeichnet (in diesem Kontext werden Fahrassistenzsysteme unter anderem als „bester Beifahrer" bezeichnet)[11]. Die Benennungsteile „aktiv" und „passiv" stammen also aus Benennungsstrategien, die mit unterschiedlichen Modellen besetzt sind (Risikomodell, Partnermodell).



10 Stieniezka 2006.
11 Vgl. www.bester-beifahrer.de.





4.6 WISSENSSCHEMATA UND KOMMUNIKATIONSMUSTER

Die Darstellung von Wissen in Form von Konzepten (kognitiv-psychologischer Terminus) und Begriffen (linguistischer Terminus) ist seit der sogenannten pragmatischen Wende (achtziger Jahre) unter verschiedenen Aspekten behandelt worden. Für diese Sicht auf Wissen bietet der Schema-Ansatz eine geeignete Darstellungsweise.[12] Hier geht es um das Miteinander-Vorkommen von Kategorien in bestimmten Kontexten und Kommunikationssituationen. Im Kontext dieses Beitrags interessieren weiterhin die Ansätze zur Fachkommunikation.[13] Eine Verbindung zwischen Begriffen und ihrer Verwendung bei der Ausführung sprachlicher Handlungen wird eher indirekt hergestellt.[14] Auch spricht man häufiger von „Textfunktionen" als von „sprachlichen Handlungen".[15] Empirische Untersuchungsmethoden (Fragebogen, Interview) können die Textanalysen ergänzen.[16]




Für die Untersuchung der Beziehungen zwischen Sicherheitsmodellen und Mustern, in denen sie kommuniziert werden, eignen sich insbesondere ausgewählte Situationen im Rahmen der Experten-Nichtexperten-Kommunikation.[17] Hierzu kann vorausgesetzt werden, dass die Beteiligten von unterschiedlichen Wissensmodellen ausgehen, ohne dass dies von vornherein offensichtlich wird. In der Rolle der Experten versprechen sie Sicherheit, in der Rolle der Nicht-Experten erwarten sie Sicherheit.[18] Vom Wissensstand her sind Nicht-Experten zugleich Experten in anderen Sachbereichen und/oder bringen als „Experten des Alltags"[19] sach- und emotionsbezogene Erfahrungen ein. Sie sind also nicht „leer", wie im Containermodell der Kommunikation suggeriert wird, sondern bringen Wissensbestände aus verschiedenen Bereichen mit, die sich auf den Verlauf der konkreten Kommunikationssituation und die Entwicklung eines transformierten Sicherheitsmodells auswirken.[20]

---

12 Vgl. Konerding 1993; Schnotz 1994; Wendt 1997.

13 Einen Überblick bieten Roelcke 2005 und Schubert 2007. Zwei Linien sind zu unterscheiden: die lexikalisch orientierte Terminologieforschung (Budin 1996; zur Technischen Dokumentation vgl. Hennig/Tjarks-Sobhani 2008) und die pragmatische Textlinguistik (Grundlagen in Heinemann/Heinemann 2002 und Brinker 2005, zu Risikowissen vgl. Rothkegel/Villiger 2005).

14 Schröder 2003.

15 Brinker 2005.

16 Brosius 2005.

17 Rothkegel 2000 und 2008.

18 Thalmann 2005.

19 Hörning 2001.

20 Die Merkmale zum alltagssprachlichen Begriff der Sicherheit, wie sie in den gängigen Wörterbüchern aufgeführt sind, geben darüber Aufschluss. Der Duden (Bedeutungswörterbuch 2002) enthält folgende Lesarten: 1. Sichersein vor Gefahr oder Schaden; 2. Gewissheit, Bestimmtheit; 3. Zuverlässigkeit; 4. Gewandtheit. Bei Klappenbach/Steinitz 1974 sind aufgeführt: 1. das Ungefährdetsein, das Geschütztsein vor Gefahr; 2. Zuverlässigkeit, Verlässlichkeit, Freisein von Fehlern, Perfektion; 3. Gewissheit, Bestimmtheit; 3. Selbstsicherheit; 4. Garantie. Im Wahrig 1973 werden genannt: 1. das Sichersein, Gewissheit; sichere Beschaffenheit, Festigkeit; Ruhe, Sorglosigkeit; Geborgenheit, Geschütztsein, Schutz; 2. Bürgschaft, Pfand; im Wahrig 2006: 1. Gewissheit, sichere Beschaffenheit; 2. Bürgschaft, Pfand.





4.7 EMPIRISCHER ANSATZ

Als empirische Basis kommen schriftlich fixierte Texte und Dialoge in Betracht, die in drei verschiedenen Kontexten angesiedelt sind:

1. Texte mit Bezug zur Mensch-Technik-Interaktion,
2. Texte mit Bezug zur Kommunikation zwischen Forschung und Behörden,
3. Texte im öffentlichen Diskurs (Medien).

Der methodische Zugriff bezieht sich auf das linguistische Instrumentarium der Text- und Dialoganalyse.[21] Innerhalb dieses Rahmens werden Kommunikationsmuster als kommunikative Handlungsmuster erfasst und in die Wissensinhalte eingebunden.[22] Die theoretischen Grundlagen sind durch die Sprechakttheorie gegeben. Von besonderem Interesse sind Muster des kommunikativen Handlungsfeldes Warnen und Drohen, die mit Handlungsanweisungen verbunden sind. Die Hypothese ist, dass in diesem Bereich Risikomodelle mit dem Paradigma Eintrittswahrscheinlichkeit und Schadensschwere oder Gewinn und Verlust angewendet werden. Dem gegenüber steht das Handlungsfeld des Versprechens, welches die Motivation zum Handeln liefert. Hier, so die Hypothese, kommt eher ein Maßnahmenmodell als Basis in Betracht, wobei Gelingensbedingungen wie Realisierbarkeit, Erwünschtheit, Ehrlichkeit und der Blick auf Maßnahmen in der Zukunft eine Rolle spielen. Die Kommunikationsmuster können deskriptiv, narrativ, instruktiv, explikativ, evaluativ oder argumentativ ausgeführt sein.

Als Ergebnis der empirischen Analysen (Dokumente im Print- und Onlineformat, Recherche, Interviews, Fragebögen) wird eine Typologie von Kommunikationsmustern im Bereich der Sicherheitskommunikation angestrebt. In einer solchen Typologie werden die semantischen Relationen zwischen den Merkmalen der jeweiligen Sicherheitsmodelle und den Parametern ihres Gebrauchs transparent. In dieser Form können sie systematisiert in einem Thesaurus und umgesetzt in webbasierte Sicherheits-Wikis öffentlich zur Verfügung gestellt werden.

4.8 LITERATUR

Arntz/Picht/Mayer 2004
Arntz, R./Picht, H./Mayer, F. (Hrsg.): Einführung in die Terminologiearbeit, Hildesheim: Olms 2004.

Banse/Bechmann 1998
Banse, G./Bechmann, G.: Interdisziplinäre Risikoforschung. Eine Bibliographie, Opladen: Westdeutscher Verlag, 1998.



21 Fritz/Hundsnurscher 1994.
22 Searle 1969; vgl. „Unglücksfälle" als Nicht-Gelingen von Sprechakten in Anlehnung an Austin (1962) in Staffeldt 2008.





Brinker 2005
Brinker, K.: Linguistische Textanalyse. Eine Einführung in Grundbegriffe und Methoden, 6. Aufl. Berlin: Schmidt, 2005.

Brosius 2005
Brosius, H. B.: Methoden der empirischen Kommunikationsforschung. Eine Einführung, Wiesbaden: Verlag für Sozialwissenschaften, 2005.

Budin 1996
Budin, G.: Wissensorganisation und Terminologie. Tübingen: Narr, 1996.

Duden 2002
Dudenredaktion (Hrsg.): Bedeutungswörterbuch, 3. Aufl. Mannheim: Dudenverlag, 2002.

Ehlich 2007
Ehlich, K.: Sprache und sprachliches Handeln, Berlin: De Gruyter 2007.

Fritz/Hundsnurscher 1994
Fritz, G./Hundsnurscher, F. (Hrsg.): Handbuch der Dialoganalyse, Tübingen: Niemeyer, 1994.

Gerzymisch-Arbogast 1996
Gerzymisch-Arbogast, H.: Termini im Kontext. Verfahren zur Erschließung und Übersetzung der textspezifischen Bedeutung von fachlichen Ausdrücken, Tübingen: Narr, 1996.

Göpferich/Schmitt 1996
Göpferich, S./Schmitt, P. A.: „Begriff und adressatengerechte Benennung: Die Terminologiekomponente beim Technical Writing.“ In: Krings, Hans (Hrsg.): Wissenschaftliche Grundlagen der Technischen Kommunikation, Tübingen: Narr, S. 369-402.

Heinemann/Heinemann 2002
Heinemann, M./Heinemann, W. (Hrsg.): Grundlagen der Textlinguistik, Tübingen: Niemeyer, 2002.





Hennig/Tjarks-Sobhani 2008
Hennig, J./Tjarks-Sobhani, M. (Hrsg.): Terminologiearbeit für Technische Dokumentation, Lübeck: Schmidt-Römhild, 2008.

Hörning 2001
Hörning, K. H.: Experten des Alltags. Die Wiederentdeckung des praktischen Wissens, Weilerswist: Velbrück Wissenschaft, 2001.

Hoffmann et al. 1998
Hoffmann, L./Kalverkämper, H./Wiegand, H. (Hrsg.): Ein internationales Handbuch zur Fachsprachenforschung und Terminologiewissenschaft, Berlin: de Gruyter, 1998.

Johnson-Laird 1983
Johnson-Laird, P.: Mental models: towards a cognitive science of language. Inference, and conscieousness, Cambridge MA: Harvard University Press, 1983.

King 2008
King, B. E.: Finding the Concept, Not just the Word: A Librarian's Guide to Ontologies, Oxford: Chandos, 2008.



Klappenbach/Steinitz 1974
Klappenbach, R./Steinitz, W.: Wörterbuch der deutschen Gegenwartssprache, Berlin: Akademie Verlag, 1974.

Konerding 1993
Konerding, K.-P.: Frames und lexikalisches Bedeutungswissen, Tübingen: Niemeyer, 1993.

Kutzner 1991
Kutzner, M.: Mentale Konstruktion von Begriffen, Frankfurt: Lang, 1991.

Liebert 2003
Libert, W.-A.: „Zu einem genetischen Konzept von Schlüsselwörtern." In: Zeitschrift für Angewandte Linguistik 38 (2003), S. 57-83.

Löbner 2003
Löbner, S.: Semantik. Eine Einführung, Berlin: de Gruyter, 2003.





Rothkegel 2000
Rothkegel, A.: „Transfer of knowledge in cross-cultural discourse." In: Jarvella, R./ Lundquist, L. (Hrsg.): Language, Text, and Knowledge, Berlin: Mouton, de Gruyter, 2000, S. 189-206.

Rothkegel 2008
Rothkegel, A.: „Wissenssysteme und ihre konzeptuellen Transformationen in der Experten/Nichtexperten-Kommunikation: Technikkommunikation in kultureller Perspektive." In: Rösch, O. (Hrsg.): Technik und Kultur, Berlin: Verlag News & Media, S. 48-60.

Rothkegel 2009
Rothkegel, A.: Technikkommunikation. Linguistische Grundlagen der Medien-, Wissens- und Textarbeit, Wien, Konstanz: UTB, 2009 (im Erscheinen).

Rothkegel/Villiger 2005
Rothkegel, A./Villiger, C.: „Modellierung von Risikowissen und multilinguale Textproduktion." In: Braun, S./Kohn, K. (Hrsg.): Sprache(n) in der Wissensgesellschaft, Frankfurt: Lang 2005, S. 205-212.




Schnotz 1994
Schnotz, W.: Aufbau von Wissensstrukturen. Untersuchungen zur Kohärenzbildung bei Wissenserwerb mit Texten, Weinheim: Beltz, 1994.

Schröder 2003
Schröder, T.: Die Handlungsstruktur von Texten. Ein integrativer Beitrag zur Texttheorie, Tübingen: Narr, 2003.

Schubert 2007
Schubert, K.: Wissen, Sprache, Medium, Arbeit. Ein integratives Modell der ein- und mehrsprachigen Fachkommunikation, Tübingen: Narr, 2007.

Searle 1969
Searle, J. R.: Speech Acts, Cambridge: Cambridge University Press, 1969. (Deutsch: Sprechakte, Frankfurt/Main: Suhrkamp, 1971.)

Sommerfeldt 2008
Sommerfeldt, K.-E.: Bezeichnungen im Umkreis des Menschen und ihr Wandel, Frankfurt: Lang, 2008.



Staffeldt 2008
Staffeldt, S.: Einführung in die Sprechakttheorie, Tübingen: Stauffenburg, 2008.

Stieniezka 2006
Stieniezka, N.: Das „narrensichere" Auto. Die Entwicklung passiver Sicherheitstechnik in der Bundesrepublik Deutschland, Darmdtadt: Wissenschaftliche Buchgesellschaft, 2006.

Thalmann 2005
Thalmann, A. T.: Risiko Elektrosmog. Wie ist Wissen in der Grauzone zu kommunizieren? Weinheim: Beltz, 2005.

Villiger 2008
Villiger, C.: „Schlüsselwörter zum Wissen: Mehrsprachige Terminologie kooperatiiv erstellen und nutzen." In: Sprache und Datenverarbeitung (2008), Nr. 2, S. 9-26.

Wahrig 1973
Wahrig, G.: Deutsches Wörterbuch, 1. Aufl. Gütersloh: Bertelsmann, 1973.




Wahrig 2006
Wahrig-Redaktion: Die deutsche Rechtschreibung, München: Wissen Media Verlag (vormals Bertelsmann), 2006.

Wendt 1997
Wendt, S.: Terminus – Thesaurus – Text. Theorie und Praxis von Fachbegriffssystemen und ihrer Repräsentation in Fachtexten, Tübingen: Narr, 1997.

Ziem 2008
Ziem, A.: Sprachliches Wissen und Frames. Kognitive Aspekte der semantischen Kompetenz, Berlin: de Gruyter, 2008.



5 GESELLSCHAFTLICHE VORAUSSETZUNGEN UND FOLGEN DER TECHNISIERUNG VON SICHERHEIT

THOMAS WÜRTENBERGER/STEFFEN TANNEBERGER

5.1 EINLEITUNG

Die Wahrung innerer Sicherheit gehört zu den traditionellen[1] und unverzichtbaren Staatsaufgaben. Staatlichkeit legitimiert sich durch den Schutz der Bürger vor inneren und äußeren Gefahren.[2] Durch den Wandel in den Bedrohungs- und Gefährdungsszenarien wird der Staat derzeit und künftig vor neue Herausforderungen gestellt, die den Einsatz neuer technischer Möglichkeiten zur Gewährleistung innerer Sicherheit nahelegen. Die Szenarien sind bekannt: grenzüberschreitende organisierte Kriminalität, nationaler und internationaler Terrorismus,[3] Gefährdung der kritischen Infrastruktur,[4] also der vielfältigen Versorgungs- und Kommunikationsnetze, sowie Zunahme von Naturkatastrophen aufgrund des Klimawandels.

Die Technisierung spielt in diesem Zusammenhang eine ebenso zentrale wie ambivalente Rolle: Neben ihrer Funktion als staatliches Instrument zur Gewährleistung innerer Sicherheit gehen vom allgemeinen technischen Fortschritt auch neue Gefahren für die innere Sicherheit aus. Dementsprechend ist zu unterscheiden zwischen solchen technischen Möglichkeiten, die eine effektivere Bekämpfung überkommener Phänomene der Gefährdung innerer Sicherheit gewährleisten sollen, und solchen, die erforderlich werden, um infolge der Technisierung erst neu entstandenen Gefährdungen auf Augenhöhe begegnen zu können.

Die neuen Techniken zur Wahrung innerer Sicherheit haben das Potenzial, gesellschaftliche Strukturen zu verändern – etwa durch neue Formen staatlicher oder gesellschaftlicher Kontrolle.[5] Die neuen Möglichkeiten der geheimen Überwachung von Wohnraum und Kommunikation sowie der Tätigkeit am Arbeitsplatz bedrohen jene Privatheit, die vom Staat und anderen gesellschaftlichen Akteuren zu achten seit jeher gefordert wird. Die Vernetzung von Systemen der Datenverarbeitung, die Beobachtung

---

1 Conze 1984, S. 831 ff. (zur „securitas" in der Römischen Kaiserzeit), S. 842 („Sicherheit" als einer der „Hauptbegriffe des europäischen Staatensystems und seines Völkerrechts").

2 Vgl. zur naturrechtlichen Begründung der Staatsaufgabe innere Sicherheit bei Hobbes, Pufendorf, Locke, Wolff, Vattel oder Bielfeld zusammenfassend Conze 1984, S. 845 ff.

3 Verwiesen sei lediglich auf Graulich 2007.

4 Vgl. hierzu Deye 2009.

5 Hirsch 2008.





im öffentlichen Raum durch Kameras, Flugroboter oder andere Methoden der Fernerkennung sowie Systeme zur Erkennung abweichenden Verhaltens verändern auf längere Sicht Verhaltensgewohnheiten und die Freiheitlichkeit unserer Gesellschaft.

Die rasch voranschreitende technische Innovation im Sicherheitsbereich und die damit verbundenen gesellschaftlichen Wandlungsprozesse führen zu neuen Herausforderungen, deren rechtliche Bewältigung in Gegenwart und Zukunft bisweilen schlagwortartig mit dem Begriff der „neuen Sicherheitsarchitektur“[6] umrissen wird. Diese Begriffbildung darf nicht darüber hinwegtäuschen, dass es inhaltlich in Politik und Wissenschaft an konzeptionellen Entwürfen fehlt und insbesondere die Frage ungeklärt ist, welche neuen Techniken in eine „neue Sicherheitsarchitektur“ integriert werden sollen und können.

Aus diesem Grund muss die technische und organisatorische Seite der Sicherheitsforschung durch eine breite sozial- und geisteswissenschaftliche Forschungsflanke ergänzt werden. Sicherheitsforschung darf sich nicht auf rein technische Aspekte bescheiden, sondern muss von Anfang an in einen gesellschaftlichen und rechtlichen Kontext eingebettet werden.





Hierbei erschließt sich ein weitgehend neues, interdisziplinäres Forschungsfeld, das Voraussetzungen und Folgefragen der Technisierung in den Blick nimmt und Optionen für eine künftige Sicherheitsarchitektur entwickelt. Breite und Tiefe dieses neuen Forschungsfeldes sollen anhand von zehn möglichen Themen entwickelt werden.

5.2 DIE AKZEPTANZ UND LEGITIMATION VON NEUEN SICHERHEITSTECHNOLOGIEN

5.2.1 BEDEUTUNG DER GESELLSCHAFTLICHEN AKZEPTANZ NEUER TECHNOLOGIEN

Neue Sicherheitstechniken werden sich nur durchsetzen, wenn sie auf gesellschaftliche Akzeptanz stoßen und, insbesondere bei staatlichem Einsatz, demokratisch legitimiert sind. Das Beispiel des sogenannten „Nacktscanners“[7] vor einigen Monaten hat in aller Deutlichkeit gezeigt, dass neue Technologien gegen einen breiten Widerstand in der öffentlichen – oder wohl treffender: veröffentlichten – Meinung nicht durchsetzbar sind. Für die Sicherheitsforschung ist daraus folgende Konsequenz zu ziehen: Angewandte Sicherheitsforschung, die in marktfähige Produkte münden soll, ist nur insoweit sinnvoll, als die neuen Sicherheitstechnologien auf gesellschaftliche Akzeptanz stoßen.

[6] Ziercke 2002; Reiter 2007; Stümper 2009; Hansen 2009.

[7] Hingewiesen sei darauf, dass der Einsatz dieser neuen technischen Möglichkeit entgegen der falschen öffentlichen Wahrnehmung nur als alternative Form der Zugangskontrolle auf freiwilliger Basis geplant war. Ebenso sollte ein Intimschutz durch technische Maßnahmen gewährleistet sein. Die gleichwohl ausgebrochene Hysterie liefert indes eindrucksvolles Anschauungsmaterial für die Macht der Medien, die mittels der suggestiven Begriffsbildung ein neues sicherheitstechnisches Instrument völlig zu diskreditieren vermochten.





Das Thema der Akzeptanz von Sicherheitstechnik ist bislang allerdings, soweit ersichtlich, noch nicht Gegenstand eingehender sozialwissenschaftlicher Forschung mit den erforderlichen empirischen Erhebungen gewesen. In diesem Forschungsfeld geht es unter anderem darum, dem anthropologisch tief verwurzelten Sicherheitsbedürfnis des Menschen nachzugehen, mögliche Diskrepanzen zwischen gefühlter und objektiver Sicherheitslage aufzudecken sowie die Erwartungen der Bürger an das notwendige Maß innerer Sicherheit und die hierfür erforderliche Bereitschaft zur Preisgabe von Privatheit herauszuarbeiten. Einzugehen wäre auch im Besonderen auf die sensible Rolle der Medien bei der Stiftung oder Verhinderung von Akzeptanz für neue Sicherheitstechnik.

So macht die in der Tendenz antiinstitutionelle Ausrichtung der Medienlandschaft besondere Sorgfalt bei der Präsentation neuer Sicherheitstechniken unabdingbar. Hier wird in der Regel die Heranziehung von Medienkompetenz zur positiven Vermittlung und Aufklärung über das neue sicherheitstechnische Instrument erforderlich sein. Denn die Frage der Akzeptanz oder Nichtakzeptanz einer neuen Technik entscheidet sich in der Praxis häufig schon bei der Frage, wie die Medien den entsprechenden Sachverhalt aufnehmen. Stößt ein bestimmtes Vorhaben auf breite Ablehnung durch die Medien, wird die veröffentlichte Meinung rasch die öffentliche Meinung in ihrem Sinne beeinflusst haben. Entscheidend wird somit sein, schon in der Kommunikation hin zu den Medien ein überzeugendes und möglichst verfälschungssicheres Gesamtkonzept zu präsentieren. Insoweit weist die sicherheitswissenschaftliche Akzeptanzforschung eine medienwissenschaftliche Dimension auf, die es zu integrieren gilt. Nur angestoßen sei in diesem Zusammenhang die Frage, inwieweit eine die Tatsachen verfälscht wiedergebende Medienkampagne auch haftungsrechtliche Folgen nach sich ziehen kann.



Weiter stellt sich die Frage, inwieweit staatlicherseits gezielt Akzeptanz für neue technische Möglichkeiten geschaffen werden kann. Wo endet zulässige staatliche Informationstätigkeit, wo beginnt die staatstheoretisch ebenso wie verfassungsrechtlich unzulässige Lenkung gesellschaftlicher Willensbildung durch staatliche Institutionen?[8]

5.2.2 GRUNDSÄTZLICHE PROBLEME DER AKZEPTANZFORSCHUNG

Wissenschaftstheoretisch ist kritisch die Frage zu stellen, ob eine sozialwissenschaftliche Akzeptanzforschung betreffs neuer Sicherheitstechnologien zu greifbaren Ergebnissen führen wird. Denn zum einen bestehen insoweit vielerlei methodische Probleme, die an dieser Stelle nicht weiter diskutiert werden sollen. Zum anderen konzentriert sich die Akzeptanzforschung in aller Regel lediglich auf den jeweiligen gesellschaftlichen Status Quo, lässt also zukünftige gesellschaftliche Entwicklungen außen vor. In der Vergangen-

8 Vgl. allgemein zu dieser staatsrechtlichen Problematik Kloepfer 2009, RN 11 ff., insbesondere RN 22.





heit konnte indessen vielfach beobachtet werden, dass bestimmte Verfahren auf dezidierte gesellschaftliche Ablehnung stießen, aber aufgrund eines kollektiven Bewusstseinswandels innerhalb weniger Jahre Akzeptanz fanden. So wurde die Überführung von Straftätern durch DNA-Analysen bis etwa 1990 dezediert abgelehnt, traf danach aber auf eine immer breiter werdende gesellschaftliche Akzeptanz und konnte schließlich in die bestehende Sicherheitsarchitektur übernommen werden (vgl. § 81 a StPO).

Zudem darf sich die Akzeptanzforschung im Hinblick auf die angestrebte globale ökonomische Verwertung neuer Sicherheitstechniken nicht auf das Inland beschränken. Vielmehr bestehen angesichts der Diversität der historischen und kulturellen Entwicklung verschiedener Gesellschaften erhebliche Unterschiede in der Akzeptanzbereitschaft, die einen europäischen und globalen Zugriff erforderlich machen. Beispielhaft sei insoweit nur auf die unterschiedliche Akzeptanz der öffentlichen Videoüberwachung in Deutschland einerseits und Großbritannien andererseits hingewiesen.

Weiter ergeben sich aus tatsächlichen Umständen Zweifel an der Leistungsfähigkeit der Aussageergebnisse der Akzeptanzforschung: Zwar ist legitimationstheoretisch anerkannt, dass die gesetzliche Normierung neuer Techniken langfristig gesehen auf gesellschaftliche Akzeptanz angewiesen ist. Andererseits wurde von politikwissenschaftlicher Seite beschrieben, dass neues Sicherheitsrecht in aller Regel eher gouvernemental denn in einem demokratischen Diskurs entwickelt wird. Dies gilt insbesondere für die Ebene der Europäischen Union, wo zu dem bekannten „Demokratiedefizit" im institutionellen Sinne ein Weiteres tritt: Aufgrund des starken Bezugs der Öffentlichkeit auf den Nationalstaat findet hier weit weniger gesellschaftliche Rückkopplung und Kritik, kurz: außerinstitutionelle Kommunikation, zwischen „Gouvernative" und Öffentlichkeit statt, als dies auf nationaler Ebene der Fall ist. In der Folge unterliegen politische Entscheidungen auf europäischer Ebene weit weniger einer Akzeptanzbindung denn auf nationaler Ebene, was die Akzeptanzforschung insoweit in ihrer Bedeutung mindert.








5.3 FREIHEIT UND SICHERHEIT

Eng mit der Akzeptanzfrage ist die Frage danach verbunden, welches Ausmaß an Freiheit und welches Ausmaß an Sicherheit ethisch und rechtlich realisiert werden sollen. Die Frage nach der „richtigen" Balance von Freiheit und Sicherheit wird infolge der Entwicklung neuer Sicherheitstechniken und der Veränderung der Gefährdungslagen beständig aufs Neue gestellt. Es handelt sich hier nicht um eine statisch zu treffende Entscheidung, sondern vielmehr um einen dynamischen Prozess beständigen Wandels der maßgeblichen Parameter, auf die im gesellschaftlichen, politischen und rechtlichen Diskurs Antworten zu finden sind.

Bislang wurde die Beantwortung dieser Fragen stark durch die rechtlichen Voraussetzungen – namentlich die Rechtsprechung des Bundesverfassungsgerichts (BVerfG) – determiniert. Dabei wurden neue technische Möglichkeiten an den Grundrechten gemessen, wobei sich das BVerfG bisweilen schwer tat, Änderungen in der überkommenen Sicherheitsdogmatik anzuerkennen.[9] Im Ergebnis wurde die Anwendbarkeit bestimmter Sicherheitstechnologien begrenzt oder gar ausgeschlossen. Dies gilt namentlich für die Rasterfahndung,[10] die Wohnraumüberwachung,[11] die Onlinedurchsuchung[12] und die Kfz- Kennzeichenerfassung[13]. Neue Technologien wie der Einsatz von Flugrobotern drohen vor dem Prüfstand des BVerfG gleichfalls in ihren Einsatzmöglichkeiten stark beschränkt zu werden, da auch insoweit ein Eingriff in das Recht auf informationelle Selbstbestimmung besteht, an deren Rechtfertigung das BVerfG strenge Anforderungen stellt.

Die als „Verfassungsgerichtspositivismus"[14] kritisierte, tendenziell affirmative Haltung der Verfassungsrechtswissenschaft gegenüber der Rechtsprechung des BVerfG weicht jedoch im Bereich des Sicherheitsrechts zunehmend rechtswissenschaftlicher Kritik. Verfassungsrechtsdogmatisch wird die Asymmetrie[15] zwischen Abwehrrechten und Schutzpflichten, die sich aus der Ableitung letzterer aus dem Verständnis von Grund-

---

9 Paradigmatisch ist insoweit der Gefahrenbegriff: In BVerfG 115, S. 320 ff. (Rasterfahndung) wird der überkommenen polizeirechtlichen Gefahrenschwelle de facto verfassungsrechtlicher Gehalt zugesprochen. Kritisch gegen eine solche Gleichsetzung von überkommener Polizeirechtsdogmatik und Rechtsstaatlichkeit wendet sich Schoch 2004, insbesondere S. 362: „Glaubt denn jemand im Ernst, dass wir im Geiste des Kreuzberg-Urteils des PrOVG von 1882 den Gefährdungslagen des 21. Jh. wirksam begegnen können?" Eine kritische Besprechung des „Rasterfahndungsurteils" findet sich auch bei Bausback 2006.

10 BVerfG 115, S. 320 ff.

11 BVerfG 109, S. 279 ff.

12 BVerfG 120, S. 274 ff.

13 BVerfG 120, S. 378 ff.

14 Schlink 1989, S. 163.

15 Vgl. allgemein hierzu Calliess 2006, RN 10.





rechten als objektiver Wertordnung ergeben, kritisiert.[16] Insoweit stellt sich die Frage, ob im Prinzip nicht von einer gleichberechtigten staatlichen Verpflichtung zu Achtung und Schutz der Grundrechte auszugehen ist, was sich über eine staatstheoretische Fundierung der Schutzpflichten[17] oder eines Rückgriffs auf Art. 1 I S. 2 GG[18] begründen lässt.

In gewaltenteiliger Hinsicht wird die Frage nach der Legitimation des BVerfG aufgeworfen, wesentliche politische Fragen im Sicherheitsrecht verfassungsrechtlich zu beantworten und damit dem demokratischen Gesetzgeber zu entziehen.[19] Insbesondere aus historischer Perspektive drängt sich die Frage auf, ob der Verfassung in einer gefestigten Demokratie, die die Bundesrepublik geworden ist, nicht eine stärker rahmensetzende Funktion zukommt, als dies in dem politisch und moralisch erschütterten Nachkriegsdeutschland der Fall gewesen sein mag.[20]

Aus rechtlicher Perspektive sei noch eine besondere Problematik erwähnt: Die Eingriffsdogmatik des Grundgesetzes nimmt den einzelnen Grundrechtseingriff zum Ausgangspunkt.[21] Im Umweltrecht wurde schon vergleichsweise früh die Gefahr erkannt, die von einer Vielzahl für sich genommen zulässiger Grundrechtseingriffe ausgehen kann.[22] Zunehmend gerät dieser Gesichtspunkt des sogenannten „additiven Grundrechtseingriffes“[23] auch im Sicherheitsrecht in den Blick und wurde vom Bundesverfassungsgericht bereits aufgegriffen: In BVerfG 100, S. 313 ff. (Telekommunikationsüberwachung), 107, S. 299 ff. (Auskunft über gespeicherte Verbindungsdaten), 111, S. 29 ff. (Sicherstellung und Beschlagnahme von Datenträgern), und 115, S. 320 ff.[24] (Rasterfahndung) wurden – nicht ausdrücklich so bezeichnet, aber der Sache nach[25] – Fälle der sogenannten „objektiven Kumulation“ entschieden. Hierunter sind nach der Begriffsbildung Kloepfers solche Fälle zu verstehen, in denen ein Hoheitsakt mehrere Grundrechtsträger betrifft.[26] Grundrechtsdogmatisch wurde diese „objektive Kumulation“ als Argument gegen die Verhältnismäßigkeit der Rechtsgrundlage gewertet.[27]

---

16 Frenz 2007, S. 635.
17 Grundlegend hierzu Isensee 1983, S. 34 ff.
18 Unruh 1996, S. 44.
19 Vgl. hierzu Haltern 1998 sowie Riecken 2003.
20 In diese Richtung argumentiert auch Wahl 2006, S. 29 ff.
21 Vgl. nur Pieroth/Schlink 2007, RN 195 ff.
22 Kloepfer 1983.
23 Vgl. hierzu allgemein Zippelius/Würtenberger 2008, § 19 RN 38 ff.
24 An diesem Urteil ist besonders problematisch, dass eine Kumulation nicht nur von Staatstätigkeiten, die für sich genommen Grundrechtseingriffe darstellen, vorgenommen wurde. Vielmehr wurde eine Kumulation auch zwischen einem Grundrechtseingriff und weiteren staatlichen Überwachungsmaßnahmen, die für sich genommen gerade keinen Grundrechtseingriff darstellen, angenommen.
25 So zutreffend Klement 2009, S. 46.
26 Kloepfer 1983, S. 214.
27 Vgl. beispielsweise BVerfG 100, S. 313 ff. [S. 75]; BVerfG 107, S. 299 ff. [S. 320]; BVerfG 115, S. 320 ff. [S. 347].





Das Urteil des Bundesverfassungsgerichtes in NJW 2005, S. 1338 ff. hatte indes einen Fall der sog. „vertikalen Kumulation“ zum Gegenstand, bei denen ein Grundrechtsträger Adressat mehrerer Grundrechtseingriffe – im vorliegenden Fall verschiedener strafprozessualer und verfassungsschutzrechtlicher Überwachungsmaßnahmen – ist. Das Bundesverfassungsgericht forderte insoweit eine verfahrensrechtliche Verhinderung unkoordinierter Überwachungsmaßnahmen verschiedener Behörden sowohl im Rahmen des geltenden Rechts durch die Vollzugsbehörden als auch erforderlichenfalls durch den Gesetzgeber. Diese Forderungen leiten über zu der Frage nach der Frage der Zentralisierung oder Dezentralisierung der Sicherheitsgewährleistung (vgl. unter 5.7).

In diesen Fragen der Grundrechtskumulation hat die Literatur – trotz zunehmender Auseinandersetzung mit dem Thema[28] – noch keine praktisch und dogmatisch befriedigenden Antworten gefunden. Insbesondere die Kategorie der „objektiven Kumulation“ sollte einer kritischen Würdigung unterzogen werden.

5.4 WANDLUNGEN IM BEREICH DES DATENSCHUTZES

Das Datenschutzrecht ist wegen neuer technischer Möglichkeiten der Kommunikation und Information im Umbruch begriffen.[29] Bislang wurde davon ausgegangen, dass Informationen aus tatsächlichen Gründen in der Regel unter Überwindung einer *Zugriffsschwelle* und aus rechtlichen Gründen in offenem Kontakt bei den betroffenen Bürgern erhoben werden müssen.[30] Gerade das Erfordernis der Überwindung tatsächlicher Zugriffsschwellen ermöglichte eine Grenzziehung zwischen privater und staatlicher Sphäre. Datenschutzrechtliche Fragestellungen konnten daher im Rahmen der überkommenen liberalstaatlichen Grundrechtsdogmatik – ausgehend vom richterverfassungsrechtlich entwickelten Grundrecht auf informationelle Selbstbestimmung[31] – bewältigt werden. Durch die umfangreiche bewusste oder unbewusste Preisgabe einer Vielzahl



---

28 Vgl. Kirchhof 2006; Klement 2009; Lücke 2001.
29 Vgl. hierzu Kutscha 2008.
30 Vgl. Würtenberger/Heckmann 2005, RN 559 ff.
31 BVerfG 65, S. 1 ff.





persönlicher Daten diffundiert diese oben beschriebene Zugriffsschwelle und mit ihr die Möglichkeit, datenschutzrechtliche Probleme als klassische Grundrechtsprobleme zu begreifen und zu bewältigen. Daher ist ein neues Datenschutzrecht zu schaffen, das den neuen Herausforderungen auf verschiedenen Ebenen begegnet:

- Zum einen ist zu fragen, ob und wenn ja, welche frei zugänglichen Informationen staatlicherseits gesammelt und verwertet werden dürfen. Insoweit wird wesentlich zu unterscheiden sein zwischen solchen Daten, die von den Bürgern nicht selten unbewusst, gewissermaßen als „Datenschweif" im digitalen Verkehr hinterlassen werden,[32] und solchen, die beispielsweise auf sozialen Plattformen bewusst der Öffentlichkeit zugänglich gemacht werden. Im Falle von Daten der letztgenannten Art wird wohl regelmäßig eine Verwertung der Daten zulässig sein, denn es entspricht gerade dem Bild des eigenverantwortlichen Bürgers, selbst über die Preisgabe persönlicher Daten zu bestimmen.[33] Auch erscheint es insoweit nicht angezeigt, staatlicherseits ein „Problembewusstsein" zu generieren: Andernfalls droht die paradoxe Situation, dass staatskritisch motivierter Datenschutz seinerseits die „Informationsgesellschaft" paternalistisch bevormundet. Insoweit ist ein gewandeltes Verständnis der Publizität persönlicher Lebensumstände staatlicherseits hinzunehmen.



- Zum anderen ist, insbesondere hinsichtlich des Schutzes vor privaten Dritten, der Bürger in den Stand zu versetzen, trotz seiner Einbindung in die neue „überwachungsgeneigte Infrastruktur"[34] selbstverantwortlich darüber zu entscheiden, welche persönlichen Daten ubiquitär verfügbar sind. Aus verfassungsdogmatischer Perspektive ist insoweit an die staatlichen Schutzpflichten zu erinnern. Diese können es gebieten, Private zur effektiven technischen Sicherung der ihnen anvertrauten Daten zu verpflichten. Weiter ist allgemein festzuhalten, dass das Datenschutzrecht durch eine intelligente Technik begleitet werden muss. Es sind Techniken zu entwickeln, die den gebotenen Freiheitsschutz in das technische System integrieren. Ganz allgemein gilt der Grundsatz: Grundrechtsschutz durch technische Verfahren.



32 Vgl. zu diesen technischen Implikationen Kutscha 2008, S. 481.

33 Allerdings ist Folgendes zu beachten: Bislang wurde die Erhebung personenbezogener Daten aus „allgemein zugänglichen Quellen", vgl. beispielsweise § 19 I S. 1 PolG BW, für zulässig erachtet. Gedacht war insoweit an Daten in Telefonbüchern, Brachenverzeichnissen etc., die nur einen Einblick in einen verhältnismäßig kleinen Teilbereich der persönlichen Verhältnisse gestatten. Anders verhält es sich jedoch bei den zum Teil umfassenden Persönlichkeitsprofilen, die auf sozialen Plattformen wie zum Beispiel „studiVZ" präsentiert werden. Hier werden häufig sämtliche persönliche Verhältnisse wie Geburtsdatum, Beziehungsstatus, Schul- und Studiendaten, Freundschaften etc. bis hin zu Urlaubsfotos einem nicht selten unbegrenzten Personenkreis zugänglich gemacht. Dies lässt es zumindest als diskussionswürdig erscheinen, ob nicht trotz des informationellen Selbstbestimmungsrechts eine Beschränkung der staatlichen Auswertung dieser Daten vorzunehmen ist.

34 Hoffmann-Riem 2002, S. 498.





5.5 VERNETZUNG UND KOOPERATION IN DER EUROPÄISCHEN UNION

Zu den Leitzielen der Europäischen Union gehört die Gewährleistung von Sicherheit.[35] Das Sicherheitsforschungsprogramm der Europäischen Union versucht neue Sicherheitstechniken zu entwickeln, die die innere Sicherheit in der Europäischen Union verbessern können. Welche Forschungsergebnisse praxistauglich sind, bleibt abzuwarten. Davon abgesehen wird durch neue Kommunikationsformen eine Vernetzung der sicherheitsrelevanten Daten, die bei den Behörden der einzelnen Mitgliedsstaaten in der Europäischen Union gespeichert sind, auf den Weg gebracht. Nach dem Prümer Vertrag[36] ist es möglich, automatisierte Anfragen nach DNA-Mustern oder Kfz-Daten grenzüberschreitend bei den Sicherheitsbehörden anderer Mitgliedsstaaten der Europäischen Union zu tätigen. Es wird ein System erarbeitet, nach dem alle sicherheitsrelevanten Daten, die in einem Mitgliedsstaat der Europäischen Union verfügbar sind, in allen Mitgliedstaaten abgefragt werden können.[37] Es versteht sich von selbst, dass derartige europaweite Vernetzungen von sicherheitsrelevanten Dateien der Mitgliedsstaaten der Europäischen Union rechtlicher Begrenzung bedürfen. Noch nicht hinreichend geklärt ist bislang, in welchem Umfang für solche Vernetzungen insbesondere datenschutzrechtliche Standards, die von den nationalen Standards abweichen, zu gelten haben,[38] ob aus Gründen nationaler Sicherheit Vorbehalte gegen die Weitergabe von Daten geltend gemacht werden können etc. Das derzeit neu entstehende europäische Sicherheitsinformationsrecht bedarf begleitender Forschung, um gemeinsame europäische Standards – unter Einbringung des deutschen Standpunktes – entwickeln zu können.




Neben der Vernetzung ist das System der Wahrung innerer Sicherheit in der Europäischen Union durch das Element der Kooperation geprägt. Dies gilt insbesondere für die Organisation der Kooperation im Bereich des Katastrophenschutzes. In der Europäischen Union wird derzeit ein Katastrophenschutz-Programm entwickelt, das sehr stark auf die Kooperation der Katastrophenschutzbehörden der einzelnen Mitgliedsstaaten der EU abstellt.[39] Zu den Leitlinien dieser Kooperation gehört, dass die jeweiligen Apparaturen und Techniken unterschiedlicher Katastrophenschutzbehörden in den einzelnen Mitgliedsstaaten der Europäischen Union anschlussfähig sind. Nur wenn technische Anschlussfähigkeit gesichert ist, kann in effektiver Weise ein länderübergreifender kooperativer Katastrophenschutz stattfinden.

---

35 Vgl. Art. 29 ff. EUV.
36 Vgl. hierzu Hummer 2007.
37 Zum Grundsatz der Verfügbarkeit vgl. Böse 2007.
38 Vgl. hierzu Würtenberger 2008, S. 39.
39 Vgl. die Mitteilung der Kommission über ein europäisches Programm für den Schutz kritischer Infrastrukturen, KOM (2006) 786 endgültig; Entscheidung 2007/779/EG, Euratom des Rates vom 08.11.2007 über ein Gemeinschaftsverfahren für Katastrophenschutz.





5.6 SICHERHEITSKOMPETENZ DER EUROPÄISCHEN UNION

Die Europäische Union hat keine supranationale Kompetenz in Sachen innerer Sicherheit. Deren Aufrechterhaltung gehört vielmehr nach wie vor zu den wesentlichen Aufgaben der Mitgliedsstaaten der Europäischen Union. Gleichwohl beansprucht die Europäische Union derzeit – vielfach gestützt auf ökonomische Gründe – eine immer weiter ausgreifende Kompetenz in Sicherheitsfragen. Jüngstes Beispiel hierfür ist die Vorratsdatenspeicherrichtlinie, die nach Auffassung des Europäischen Gerichtshofes auf Art. 95 EG – einer Kompetenzgrundlage, „welche die Errichtung und das Funktionieren des Binnenmarktes zum Gegenstand" hat – gestützt werden konnte.[40] Der EuGH betonte insoweit – ganz entgegen der genuin sicherheitspolitisch motivierten Stoßrichtung der fraglichen Richtlinie – binnenmarktspezifische Aspekte: Der Wettbewerb zwischen den Dienstanbietern dürfe nicht dadurch verfälscht werden, dass diese nur in einem Teil der Mitgliedsstaaten zu der technisch aufwändigen Vorratsdatenspeicherung verpflichtet würden. Aus diesem Grund sei die Europäische Union berechtigt, Eckpunkte für die Vorratsdatenspeicherung in allen Mitgliedsstaaten der Europäischen Union zur Herstellung von Wettbewerbsgleichheit festzulegen. Als Spill Over[41] dieser Regelungskompetenz bietet sich an und ist von der EU zudem erwünscht sowie möglicherweise durch die Dogmatik grundrechtlicher Schutzpflichten gefordert, die Vorratsdatenspeicherung sicherheitsrechtlich zu nutzen.

Punktuelle sicherheitsrechtliche Kompetenzen hat die EU im Bereich von Dienstleistungen, von Telekommunikation, des Betriebs von Flughäfen etc. durch die Einführung sicherheitsrechtlicher Standards wahrgenommen. Dies führt dazu, dass sich die nationalen Technologien sehr stark an der Standardsetzung durch die Europäische Union zu orientieren haben.

Diese bisherigen Forschungsschwerpunkte dürften sich im Falle des Inkrafttretens des Vertrages von Lissabon[42] verschieben: Denn durch diesen Vertrag findet zum einen eine Abkopplung des Raums der Freiheit der Sicherheit und des Rechts von seiner dem Binnenmarkt dienenden Funktion[43] sowie eine Ausweitung der intergouvernementalen und supranationalen Handlungsmöglichkeiten der EU statt[44]. Zum anderen werden bislang intergouvernementale Handlungsoptionen in Bezug auf den Raum der Freiheit, der

---

[40] EuGH NJW (2009), S. 1801 ff.; kritisch dazu Simitis 2009 (S. 1784: Nicht nachvollziehbar ist die Annahme des EuGH, die Vorratsdatenspeicherungsrichtlinie erfasse nicht den Zugang von Polizei- und Justizbehörden zu den gespeicherten Daten).

[41] Zum Begriff des Spill Over vgl. Neidhardt 2008, S. 16 ff.

[42] Mit dem Urteil des BVerfG vom 30. Juni 2009 (Aktenzeichen: 2 BvE 2/ 08) hat das BVerfG zum einen unmissverständliche Signale an die Adresse des EuGH ausgesandt und zum anderen eine stärkere innerstaatliche Beteiligung der gesetzgebenden Körperschaften bei faktischen Vertragserweiterungen (Stichwort: „Integrationsverantwortung") gefordert. Im Ergebnis stehen aber der Ratifikation des Vertrages in der Bundesrepublik nach dem Erlass eines den Vorgaben des BVerfG entsprechenden Begleitgesetzes keine substanziellen Hindernisse entgegen. Das weitere Schicksal des Vertrages von Lissabon hängt damit in erster Linie vom Ausgang der zweiten Volksabstimmung der Iren ab, die für Oktober 2009 anberaumt ist.

[43] So unter Berufung auf Art. 67, 77, 81, 82 AV Müller/Graff 2009, S. 111.

[44] Müller/Graff 2009, S. 114.








Sicherheit und des Rechts (vgl. Art. 34 EUV) „vergemeinschaftet".[45] Insbesondere der letzte Punkt wird die Wissenschaft dazu zwingen, dem Raum der Freiheit, der Sicherheit und des Rechts eine deutlich größere Aufmerksamkeit zu widmen als dies bislang der Fall war.

5.7 SICHERHEITSTECHNIK UND ÖKONOMISCHE RAHMENSETZUNG

Wie künftige Sicherheitstechnik aussieht, ist auch durch die ökonomischen Rahmensetzungen bestimmt. Dies betrifft zunächst den staatlichen Bereich. Neue, kostspielige Sicherheitstechnik muss haushaltsrechtlich umsetzbar sein. Dies bedeutet, dass sie sich einer detaillierten Kosten-/ Nutzenanalyse stellen muss. So muss sich eine neue Sicherheitstechnik, die beispielsweise Tunnel durch bessere Armierungen sicherer macht, darauf befragen lassen, ob die Erhöhung der Sicherheit den möglicherweise beträchtlichen Aufwand an Mehrkosten rechtfertigt.[46] Aus rechtlichem Blickwinkel ist damit die Frage nach der Stringenz staatlicher Rechtsetzung aufgeworfen, wonach – allerdings unter Anerkennung einer weiten gesetzgeberischen Einschätzungsprärogative – eine folgerichtige Kosten-/ Risikominderungsnutzen-Verteilung zu fordern sein wird. Problematisch ist insoweit, dass bestimmte Risiken – zum Beispiel aufgrund ihrer medialen Attraktivität – ein relatives Übermaß an Aufmerksamkeit erhalten, was nach der Logik der Mediendemokratie ein relatives Übermaß an Ressourcenaufwand zur Bekämpfung dieser Risiken zur Folge hat. Beispielhaft sei die Terrorabwehr in Relation zu gewöhnlichen Formen organisierter Kriminalität oder in Relation zu Gefahren, die von Naturkatastrophen ausgehen, genannt.



Äußerst schwierig gestaltet sich die angesprochene ökonomische Kosten-/ Nutzen-Wertung im konkreten Fall. Insoweit bereitet bereits die Definition des Schutzgutes, erst recht aber dessen Relation zu anderen Schutzgütern Schwierigkeiten: Ist beispielsweise das Vertrauen der Bürger in die Schutzfähigkeit des Staates vor Terroristen ein zu schützendes Gut, das es gebietet, dem Terror gegenüber anderen Risiken vorzugsweise zu begegnen? Wie stellt sich das Verhältnis des Schutzes körperlicher Integrität zum Schutz von Sachwerten dar? Oder ganz allgemein: Lassen sich überhaupt in Bezug auf

45 Hierzu Müller/Graff 2009, S. 119.

46 Allgemein zum Erfordernis stringenter staatlicher Gesetzgebung: BVerfG NJW (2008), S. 2409 ff. (Nichtraucherschutzgesetz) und NJW (2009), S. 48 ff. (Pendlerpauschale).







bestimmte Risiken tragfähige Wahrscheinlichkeitsberechungen anstellen? Diese Fragen sind bislang noch nicht geklärt, werden jedoch seit Kurzem in der Sicherheitsökonomie systematisch angegangen.[47]

Schwerpunkte der sicherheitsökonomischen Forschung sind nicht nur die direkten ökonomischen und sozialen Kosten von Terrorismus, organisierter Kriminalität oder auch von Naturkatastrophen. Es geht darüber hinaus um eine kostenmäßige Bewertung der sogenannten Kaskadeneffekte. Hierbei geht es im Kern um Sekundärschäden, die aus häufig irrationalen Verhaltensabweichungen der Bevölkerung nach erfolgtem Primärschlag resultieren. Beispiel hierfür ist der 11. September 2001, der das Passagieraufkommen für US-Binnenflüge über einen längeren Zeitraum empfindlich reduzierte, was erhebliche volkswirtschaftliche Schäden verursachte. Insoweit ist eine neue Akzentuierung der Gefahrenabwehr auszumachen: Da sich Schadensereignisse nicht mit absoluter Sicherheit verhindern lassen, sind auf sekundärer Ebene Möglichkeiten der Schadensgeringhaltung in den Blick zu nehmen. Dieser Gesichtspunkt der Schadensgeringhaltung kann aber nur einen weiteren, wenngleich wesentlichen Aspekt der Schadensabwehr darstellen. Dies ergibt sich schon aus der praktischen Erwägung, dass Sekundärschäden tendenziell Vermögensschäden, Primärschäden aber häufig auch Personenschäden sind.

Die Sicherheitsökonomie bietet ungeachtet der angedeuteten Schwierigkeiten einen Erfolg versprechenden Forschungsansatz, der zu einer Rationalisierung der bisweilen affektiv motivierten Sicherheitsanstrengungen beitragen kann. Forschungsgegenstand wird auch die Frage sein, inwieweit die erzielten Ergebnisse unter dem angesprochenen Gesichtspunkt stringenter Gesetzgebung rechtliche Konsequenzen zeitigen.

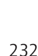


5.8 ZENTRALISIERUNG ODER DEZENTRALISIERUNG

Eine andere Frage ist, ob die neue Sicherheitsarchitektur eher zentralistisch oder dezentral aufgebaut werden soll. Derzeit geht die Tendenz dahin, durch Zentralisierung einen Beitrag zur Verbesserung innerer Sicherheit zu gewährleisten. Dies betrifft die Neuorganisation der Bundespolizei sowie den Kompetenzzuwachs des Bundeskriminalamtes. Insbesondere die Zentralisierung der Verarbeitung sicherheitsrelevanter Daten, die in den letzten Jahren zunehmend beim Bundeskriminalamt und damit beim Bund organisiert wurde,[48] führt zu einem Perspektivwechsel in der bisherigen föderal-dezentralen polizeilichen Aufgabenerfüllung.

47 Einen ersten Überblick bieten Brück/Karaisl/Schneider 2008.

48 Zur Antiterrordatei Stubenrauch 2009; kritisch Roggan 2009; einen Überblick über die Neuerungen in der deutschen Sicherheitsarchitektur seit 2001 gibt Hansen 2009, S. 87 ff.








Demgegenüber bleibt zu erwägen, ob nicht durch dezentrale und autarke Systeme ebenfalls ein Beitrag zur Optimierung innerer Sicherheit gewährleistet werden kann. Dies betrifft zunächst die Orts- und Bürgernähe der Polizei, die nicht aufgegeben werden darf. Problematisch ist zudem eine Zentralisierung der Versorgungs- und Kommunikationssysteme, die im Hinblick auf Terrorismus oder Unglücksfälle besonders störanfällig sind. Durch eine dezentrale Organisation lassen sich großflächige Netzausfälle mit immensen volkswirtschaftlichen Kosten verhindern helfen.

Insoweit zeigt sich bereits jetzt die doppelte Ambivalenz des Verhältnisses von Zentralisierung und Dezentralisation: Denn genauso wenig wie Zentralisierung mit einem Zugewinn an Sicherheit gleichgesetzt werden kann (vgl. beispielsweise die Sabotageanfälligkeit zentralisierter Versorgungseinrichtungen), führt Dezentralisierung automatisch zu einem Freiheitszugewinn (vgl. beispielsweise die Problematik kumulativer Grundrechtseingriffe bei einer starken Zersplitterung der Sicherheitsbehörden). Daher hat die Forschung die Beziehungen zwischen Dezentralisierung und Zentralisierung, Freiheit und Sicherheit im Hinblick auf einzelne Sachbereiche oder Schutzgüter herauszuarbeiten, um dadurch die tatsächlichen Voraussetzungen für die in erster Linie politisch zu treffende Frage über die Balance von Freiheit und Sicherheit zu schaffen. Es handelt sich hierbei um eine zentrale Frage der künftigen Sicherheitsarchitektur, deren Beantwortung noch aussteht.




5.9 ZERTIFIZIERUNG

In der künftigen Sicherheitsarchitektur ist nicht mehr der Staat alleiniger Garant innerer Sicherheit; vielmehr wird deren Gewährleistung in zunehmendem Umfang privatisiert.[49] Sicherheitsunternehmen und Sicherheitstechnik, die dem Einzelnen und gesellschaftlichen Gruppen Sicherheit zu gewährleisten vermögen, bilden derzeit und in Zukunft einen rasch wachsenden Markt.

Der Bürger, der auf diesem Markt Sicherheitsprodukte erwirbt, muss ihre Tauglichkeit erkennen können. Dies gilt angesichts der immer stärkeren Technisierung, beispielsweise der IT- Sicherheit, umso mehr, als hier die Wirksamkeit von erkauften Sicherheitsmaßnahmen vom Laien auch nicht nur ansatzweise beurteilt werden kann. Hier ist es Aufgabe des Staates, Qualitätsstandards festzulegen und für Transparenz in diesem neu entstandenen Markt zu sorgen.[50] Dies gilt angesichts der Bedeutung des Staatszwecks

---

49 Zu den hiergegen bestehenden Bedenken Hetzer 2000; dezidiert für ppp im Sicherheitsrecht Stober 1997; allgemein zur Privatisierung der Gefahrenabwehr Würtenberger/Heckmann 2005, RN 32.

50 Spindler, in: Deye 2009, S. 707. Hierbei ist allerdings zu beachten, dass nicht jede privat nachgefragte Sicherheitsleistung zugleich die staatliche Aufgabe der Gewährleistung innerer Sicherheit betrifft. Insofern kann von einer eigentlichen Verpflichtung des Staates zur Schaffung transparenter Märkte eigentlich auch nur für die Bereiche ausgegangen werden, bei denen staatlich gebotener Schutz durch privat erworbenen Schutz substituiert wird.





„Sicherheit" zumindest dann, wenn nicht auf andere Weise Mindeststandards und Markttransparenz geschaffen werden können. In dem Maße, in welchem sich der Staat aus der Aufgabe der Sicherheitsgewährleistung zurückzieht, muss er kompensatorisch zumindest die Rahmenbedingungen für eine funktionierende private Sicherheitsgewährleistung schaffen. Für den Bereich privater Wachdienste ist der Gesetzgeber durch die Schaffung des § 34a GewO dieser Verpflichtung ansatzweise[51] nachgekommen. Ein solcher gewerbeaufsichtsrechtlicher Zugriff ist jedoch in Bezug auf neue technische Instrumente der Sicherheitsgewährleistung nur begrenzt möglich. Dies liegt zum einen daran, dass hier, anders als im Bewachungsgewerbe, nicht die Erbringung persönlicher Dienste im Vordergrund steht. Zum anderen lassen sich die Anforderungsprofile (vgl. etwa die individuelle Erstellung einer Software zur Abwehr von Wirtschaftsspionage) nur sehr schwer durch gesetzliche Typisierungen erfassen. Daher bieten sich insoweit ökonomische Steuerungsansätze an, die, wie beispielsweise die Erteilung von Zertifikaten, grundsätzlich auf marktwirtschaftliche Selbstregulierung aufbauen, diese jedoch durch Schaffung von Transparenz und Qualitätssicherung optimieren. Hierbei handelt es sich um ein neues Forschungsfeld,[52] das sinnvollerweise Erfahrungen mit Zertifikationen in anderen Bereichen, genannt sei zum Beispiel das Ökoauditverfahren,[53] aufgreifen und ein eigenständiges Modell für technische Sicherheitsgewährleitung entwickeln müsste.




5.10 NEUES RECHT FÜR NEUE TECHNIK

Nach alter Erfahrung verlangt neue Technik nach neuem Recht. Das Technikrecht als rechtswissenschaftliches Forschungsthema muss sich zunehmend und frühzeitig der Sicherheitstechnik zuwenden. Andernfalls droht das Primat des Rechts gegenüber faktischen Entwicklungen in der Sicherheitstechnik zumindest für einen Übergangszeitraum ins Hintertreffen zu geraten. Neue technische Möglichkeiten müssen frühzeitig erkannt, diskutiert und bewältigt werden. Die Rechtsordnung hat zu regeln, welche Sicherheitstechniken zulässig sind und welche Haftungsfolgen bei Versagen von Sicherheitstechniken eintreten. Jede neue Sicherheitstechnik, die in die Privatsphäre und in das Recht auf informationelle Selbstbestimmung eingreift, ist auf den kritischen Prüfstand rechtswissenschaftlicher Analyse zu stellen. Auf der anderen Seite verhindert eine solche frühzeitige Kooperation die Erforschung technischer Instrumente, die aus rechtlichen oder – wie das bereits angesprochene Beispiel des Nacktscanners zeigt – politischen Gründen nicht zum Einsatz kommen können, und bewahrt so vor wirtschaftlichen Fehlinvestitionen. Derzeit scheint die erforderliche Abstimmung von technischen und rechtlichen

[51] Aber auch hier besteht noch erheblicher Reformbedarf. § 34a GewO stellt in erster Linie Mindestanforderungen an die Zuverlässigkeit der von Wachdiensten eingesetzten Personen. Weiter stellt sich aber das Problem, dass das freiheitssichernde öffentliche Verfahrensrecht auf private Wachdienste keine Anwendung findet. Damit kann sich der betroffene Bürger gegenüber Angehörigen eines Wachdienstes in Konfliktfällen auf rechtsstaatliche Mindeststandards nicht berufen (allenfalls kommt eine Korrektur im Rahmen der allgemeinen Rechtfertigungsgründe wie dem der Gebotenheit bei § 32 StGB in Betracht).

[52] Vgl. aber schon Schomburg/Fischer 2005, S. 1285.

[53] Vgl. allgemein hierzu Sparwasser/Engel/Voßkuhle, § 5 RN 53 ff.





Aspekten noch nicht in ausreichendem Maße vorgenommen zu werden. Beispielsweise begegnet die Beobachtung durch Flugroboter oder eine satellitengestützte Fernerkundung, wie sie derzeit von der Europäischen Union im Landwirtschaftsbereich auf den Weg gebracht wird, erheblichen verfassungsrechtlichen Bedenken.

Überdies ist der bislang vernachlässigten Frage nachzugehen, inwieweit Freiheitssphären vermittels des Einsatzes neuer Sicherheitstechniken durch Private gefährdet werden und welcher staatlicher Regelungen es hier bedarf.[54]

5.11 WANDEL DER STAATLICHKEIT

Alle skizzierten Themenfelder führen in eine neue Sicherheitsarchitektur, die von einem grundlegenden Wandel in der Staatlichkeit geprägt ist. Dabei ist es ein Gemeinplatz, dass seit dem letzten Drittel des 20. Jahrhunderts der Präventionsstaat ältere Formen eines bloß reaktiven und gegensteuernden Staates abgelöst hat.[55] Mit dieser Wendung zum Präventionsstaat verbindet sich zugleich eine Entgrenzung der Staatsaufgabe „innere Sicherheit". Brauchte der alte Nationalstaat innere Sicherheit nur innerhalb seiner territorialen Grenzen zu gewährleisten, so fordert die Globalisierung der Gefährdungslagen neue Formen zwischenstaatlicher Kooperation und Organisation. Ein weiterer Perspektivwechsel vollzieht sich von der traditionell hoheitlich zu erfüllenden Staatsaufgabe „innere Sicherheit" hin zu einer kooperativen Aufgabenbewältigung. Die auch in anderen Bereichen entwickelten Formen eines kooperativen Verwaltungsstaates begegnen uns nun im neuen Modell einer Police-Private-Partnership.[56] Innere Sicherheit zu gewährleisten kann nur in einer umfassenden Kooperation von Staat und Gesellschaft, also gemeinsam mit den Bürgern, den privaten Betreibern kritischer Infrastruktur, den privaten Sicherheitsunternehmen[57] und anderen gesellschaftlichen Organisationen, gelingen. Eine solche Teilung der Sicherheitsverantwortung führt bei der Entwicklung eines Infrastruktursicherheitsverwaltungsrechts zu der zentralen Frage, wie die Verantwortungsethik fortzuentwickeln ist. Was bedeutet es für das Menschenbild und für die Sozialethik ganz allgemein, dass im gesellschaftlichen Bereich und damit seitens jedes Einzelnen verantwortungsvoll an der Gewährleistung innerer Sicherheit mitzuwirken ist? Damit im Zusammenhang steht die weitere Grundsatzfrage: Inwieweit besteht für den Staat eine Erfüllungsverantwortung? Muss er durch Recht und damit verbunden durch Eingriff, Befehl und Zwang innere Sicherheit gewährleisten? Und inwieweit kann er sich auf eine Gewährleistungsverantwortung, also auf eine Überwachung der gesellschaftlichen und damit privaten Organisation innerer Sicherheit zurückziehen?



---

[54] Vgl. hierzu schon die Ausführungen unter 5.3.
[55] Würtenberger/Heckmann 2005, RN 33 ff.
[56] Vgl. Würtenberger/Heckmann 2005, RN 32; Pitschas 2004.
[57] Vgl. hierzu Schäuble, in: Deye 2009.





Ob diese und andere Fragestellungen lediglich Wandlungsprozesse oder Paradigmenwechsel in der Staatlichkeit betreffen, lässt sich an dieser Stelle nicht weiter vertiefen. Eines jedenfalls sollte deutlich gemacht werden: Wie die Sicherheitsarchitektur des für eine supra- und internationale Kooperation offenen, an Prävention und gesellschaftlicher Mitwirkung orientierten Staates aussehen wird – vor allem, welche Optionen sie wählen wird – gehört zu den zentralen Forschungsfragen der Zukunft.

5.12 LITERATURVERZEICHNIS

Bausback 2006
Bausback, W.: „Fesseln für die wehrhafte Demokratie?" In: NJW (2006), S. 1922 ff.

Böse 2007
Böse, M.: Der Grundsatz der Verfügbarkeit von Informationen in der strafrechtlichen Zusammenarbeit der Europäischen Union, Göttingen: V & R Unipress, 2007.

Brück/Karaisl/Schneider 2008
Brück, T./Karaisl, M./Schneider, F.: "A Survey on the Economics of Security." In: DIW Berlin (Hrsg.): Politikberatung kompakt 41 (April 2008).

Calliess 2006
Calliess, C.: „§ 44 – Schutzpflichten." In: Merten, D., Papier, H.-J. (Hrsg.): Handbuch der Grundrechte in Deutschland und Europa, Band II: Grundrechte in Deutschland - Allgemeine Lehren I, Heidelberg: C.F. Müller, 2006.

Conze 1984
Conze, W. „Sicherheit, Schutz." In: Brunner, O./Conze, W./Koselleck, R. (Hrsg.): Geschichtliche Grundbegriffe, Bd. 5, Stuttgart: Klett, 1984.

Deye 2009
Deye, S.: Schutz kritischer Infrastrukturen – IT und Energie, (Tagungsbericht), In: DVBl (2009), S. 706 f.

Frenz 2007
Frenz, W.: „Menschenwürde und Persönlichkeitsschutz versus Opferschutz und Fahndungserfolg." In: NVwZ (2007), S. 631 ff.

Graulich 2007
Graulich, K. (Hrsg.): Terrorismus und Rechtsstaatlichkeit, Berlin: Akademie-Verlag, 2007.





Haltern 1998
Haltern, U. R.: Verfassungsgerichtsbarkeit, Demokratie und Misstrauen, Berlin: Duncker und Humblot, 1998.

Hansen 2009
Hansen, S.: Neue deutsche Sicherheitsarchitektur, Frankfurt/Main: Lang, 2009.

Hetzer 2000
Hetzer, W.: „Ökonomisierung der Inneren Sicherheit? – Rechtsgüterschutz zwischen Staat und Gewerbe." In: ZRP (2000), S. 20 ff.

Hirsch 2008
Hirsch, B.: „Gesellschaftliche Folgen staatlicher Überwachung." In: DuD (2008), S. 87 ff.

Hoffmann-Riem 2002
Hoffmann-Riem, W.: „Freiheit und Sicherheit im Angesicht terroristischer Anschläge." In: ZRP (2002), S. 479 ff.

Hummer 2007
Hummer, W.: „Der Vertrag von Prüm – ‚Schengen III'?" In: EuR (2007), S. 521 ff.

Isensee 1983
Isensee, J.: Das Grundrecht auf Sicherheit, Berlin: de Gruyter, 1983.

Kirchhof 2006
Kirchhof, G.: „Kumulative Belastungen durch unterschiedliche staatliche Maßnahmen." In: NJW (2006), S. 732 ff.

Klement 2009
Klement, J. H.: „Die Kumulation von Grundrechtseingriffen." In: AöR (2009), S. 35 ff.

Kloepfer 1983
Kloepfer, Michael: „Belastungskumulationen durch Normüberlagerungen im Abwasserrecht." In: VerwArch (1983), S. 210 ff.

Kloepfer 2005
Kloepfer, M.: „§ 42 – Öffentliche Meinung, Massenmedien." In: Handbuch des Staatsrechts III, 3. Aufl. Heidelberg: C.F. Müller, 2005.





Kutcha 2008
Kutscha, M.: „Überwachungsmaßnahmen von Sicherheitsbehörden im Fokus der Grundrechte." In: LKV (2008), S. 481 ff.

Lücke 2001
Lücke, J.: „Der additive Grundrechtseingriff und das Verbot übermäßiger Gesamtbelastung des Bürgers." In: DVBl (2001), S. 1469 ff.

Müller-Graff 2009
Müller-Graff, P.-C.: „Der Raum der Freiheit, der Sicherheit und des Rechts in der Lisabonner Reform." In: Schwarze, J./Hatje, A. (Hrsg.): Der Reformvertrag von Lissabon, Baden-Baden: Nomos, 2009, S. 105 ff.

Neidhardt 2008
Neidhardt, S.: Nationale Rechtsinstitute als Bausteine europäischen Verwaltungsrechts, Tübingen: Mohr Siebeck, 2008.

Pieroth/Schlink 2007
Pieroth, B./Schlink, B.: Grundrechte – Staatsrecht II, 23. Aufl. Heidelberg: C.F. Müller, 2007.

Pitschas 2004
Pitschas, R.: „Neues Verwaltungsrecht im partnerschaftlichen Rechtsstaat?" In: DÖV (2004), S. 231 ff.

Reiter 2007
Reiter, H.: „Die neue Sicherheitsarchitektur der NATO." In: Kritische Justiz (2007), S. 124 ff.

Riecken 2003
Riecken, J.: Verfassungsgerichtsbarkeit in der Demokratie, Berlin: Duncker und Humblot, 2003.

Roggan 2009
Roggan, F.: „Das neue BKA-Gesetz – Zur weiteren Zentralisierung der deutschen Sicherheitsarchitektur." In: NJW (2009), S. 257 ff.





Schlink 1989
Schlink, B.: „Die Entthronung der Staatsrechtswissenschaften durch die Verfassungsgerichtsbarkeit." In: Der Staat (1989), S. 161 ff.

Schoch 2004
Schoch, F.: „Abschied vom Polizeirecht des liberalen Rechtsstaates?" In: Der Staat (2004), S. 347 ff.

Schomburg/Fischer 2005
Schomburg, B./Fischer, C.: „Das Sicherheitsgewerbe und der europäische Binnenmarkt – Chancen und Risiken – Tagungsbericht des 6. Sicherheitsgewerberechtstages." In: NVwZ (2005), S. 1284 ff.

Simitis 2009
Simitis, S.: „Der EuGH und die Vorratsdaten oder die verfehlte Kehrtwende bei der Kompetenzregelung." In: NJW (2009), S. 1782 ff.

Sparwasser/Engel/Voßkuhle 2003
Sparwasser, R./Engel, R./Voßkuhle, A.: Umweltrecht, 5. Aufl. Heidelberg: C.F. Müller, 2003.

Stober 1997
Stober, R.: „Staatliches Gewaltmonopol und privates Sicherheitsgewerbe – Plädoyer für eine Police-Private-Partnership." In: NJW (1997), S. 889 ff.

Stubenrauch 2009
Stubenrauch, J.: Gemeinsame Verbunddateien von Polizei und Nachrichtendiensten, Baden-Baden: Nomos, 2009.

Stümper 2009
Stümper, A.: „Sicherheitsarchitektur von Heute – total überholt." In: Die Polizei (2009), S. 93 ff.

Unruh 1996
Unruh, P.: Zur Dogmatik der grundrechtlichen Schutzpflichten, Berlin: Duncker und Humblot, 1996.





Wahl 2006
Wahl, R.: Herausforderungen und Antworten: Das Öffentliche Recht der letzten fünf Jahrzehnte, Berlin: De Gruyter, 2006.

Würtenberger/ Heckmann 2005
Würtenberger, T./Heckmann, D.: Polizeirecht in Baden-Württemberg, 6. Aufl. Heidelberg: C.F. Müller, 2005.

Würtenberger 2008
Würtenberger, T.: „Polizei- und Sicherheitsrecht vor den Herausforderungen des Terrorismus – eine deutsche Perspektive." In: Masing, J./Jouanjan, O. (Hrsg.): Terrorismusbekämpfung, Menschenrechtsschutz und Föderation, Tübingen: Mohr Siebeck, 2008.

Ziercke 2002
Ziercke, J.: „Neue Sicherheitsarchitektur für Deutschland." In: Kriminalistik (2002), S. 346 ff.

Zippelius/ Würtenberger 2008
Zippelius, R./Würtenberger, T.: Deutsches Staatsrecht, 32. Aufl. München: C.H. Beck, 2008.








> AUSBILDUNG FÜR MEHR SICHERHEITSKOMPETENZ



1 KOMPETENZEN FÜR DIE SICHERHEIT

NORBERT PFEIL/WOLFRAM RISCH

1.1 EINLEITUNG

Der vorliegende Beitrag schafft ein begriffliches Dach für zwei unterschiedliche, beispielhafte Herangehensweisen an die Frage, welche Kompetenzen für die Gewährleistung von Sicherheit auf welche Weise zu schaffen bzw. zu erhalten sind. Die Begriffe „Sicherheit" und „Kompetenz" werden zu diesem Zweck für sich in ihrer Bedeutung beleuchtet.

1.2 SICHERHEIT

Der Begriff „Sicherheit" soll hier nicht in seiner gesamten gesellschaftlichen Dimension ausgeleuchtet, sondern vielmehr pragmatisch in dem in Deutschland verbreiteten technischen Begriffsverständnis nach der zurückgezogenen, aber noch häufig zitierten DIN-Norm DIN VDE 31000 Teil 2[1] verwendet werden. Die Nachfolgenorm DIN 820-120[2] steht diesem Begriffsverständnis nicht entgegen. Dass Sicherheit einen hohen Stellenwert in der Bedürfnishierarchie des Menschen hat, muss hier nicht näher ausgeführt werden (Sicherheit folgt in der Maslowschen Bedürfnishierarchie direkt der Befriedigung der körperlichen Grundbedürfnisse)[3].

Das Begriffsverständnis für Sicherheit nach DIN VDE 31000 Teil 2 basiert auf den Begriffen „Risiko" und „Grenzrisiko". Nachfolgend sind die relevanten Begriffsbestimmungen dieser Norm aufgeführt.

Risiko: Das Risiko, das mit einem bestimmten technischen Vorgang oder Zustand verbunden ist, wird zusammenfassend durch eine Wahrscheinlichkeitsaussage beschrieben, die

- die zu erwartende Häufigkeit eines zum Schaden führenden Ereignisses und
- das beim Ereigniseintritt zu erwartende Schadensausmaß

berücksichtigt.

---

1 DIN 1987.
2 DIN 2008.
3 Maslow 1943.





Schaden: Schaden ist ein Nachteil durch Verletzung von Rechtsgütern aufgrund eines bestimmten technischen Vorgangs oder Zustands.

Grenzrisiko: Grenzrisiko ist das größte noch vertretbare Risiko eines bestimmten technischen Vorgangs oder Zustands. Im Allgemeinen lässt sich das Grenzrisiko nicht quantitativ erfassen. Es wird in der Regel indirekt durch sicherheitstechnische Festlegungen beschrieben.

Gefahr: Gefahr ist eine Sachlage, bei der das Risiko größer als das Grenzrisiko ist. Sicherheit: Sicherheit ist eine Sachlage, bei der das Risiko kleiner als das Grenzrisiko ist.

Schutz: Schutz ist die Verringerung des Risikos durch Maßnahmen, die entweder die Eintrittswahrscheinlichkeit oder das Ausmaß des Schadens oder beides einschränken.

Abbildung 1: Zusammenhang zwischen Risiko, Grenzrisiko, Sicherheit und Gefahr (Begriffe zum Risiko nach DIN VDE 31000 Teil 2)



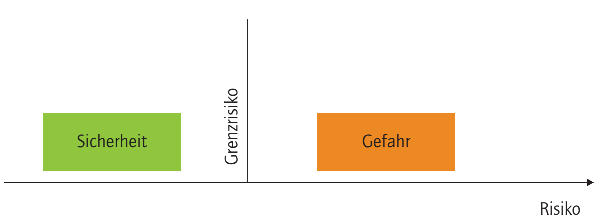




Abbildung 1 verdeutlicht den Zusammenhang zwischen Risiko, Grenzrisiko, Sicherheit und Gefahr. „Sicherheit" bedeutet also weder, dass der Eintritt eines Schadens unter keinen Umständen möglich ist, noch bedeutet „Gefahr", dass ein Schaden eintreten muss. Der Verständigung auf ein – gesellschaftlich akzeptiertes – Grenzrisiko und dessen Einhaltung kommt daher eine entscheidende Rolle zu. Voraussetzung dafür ist, dass die mit den betrachteten Vorgängen oder Zuständen verbundenen Risiken ausreichend bekannt und zumindest qualitativ beschreibbar sind, als Grundlage für alle weiteren Festlegungen wie beispielsweise zu Schutzmaßnahmen.



Als Beispiel für eine diesbezügliche methodische Vorgehensweise wird auf die Beurteilung der Arbeitsbedingungen nach § 5 Abs. 1 Arbeitsschutzgesetz[4] verwiesen, wo es heißt: „Der Arbeitgeber hat durch eine Beurteilung der für die Beschäftigten mit ihrer Arbeit verbundenen Gefährdung zu ermitteln, welche Maßnahmen des Arbeitsschutzes erforderlich sind." Dieses zentrale Element des betrieblichen Arbeitsschutzes erfordert eine systematische Beurteilung der für die Beschäftigten mit ihrer Arbeit verbundenen Gefährdungen und Belastungen (Gefährdungsbeurteilung), mit den Schritten:

- Gefährdungen ermitteln,
- Gefährdungen bewerten (durch Vergleich mit dem sicheren bzw. gesundheitsgerechten Sollzustand) und (erforderlichenfalls)
- Maßnahmen ableiten, durchführen und deren Wirksamkeit überprüfen.[5]

Diese für den Arbeitsschutz skizzierte Vorgehensweise gilt für die Gewährleistung von Sicherheit in anderen Bereichen in entsprechender Weise und erfordert in den jeweiligen Bereichen entsprechende fachliche Kompetenzen.



1.3 KOMPETENZ

Unter „Kompetenzen" werden messbare Muster an Wissen, Fähigkeiten, Fertigkeiten, Motivation und Verhaltensweisen verstanden, die eine Person für die erfolgreiche Bewältigung ihrer Aufgaben benötigt. Komponenten jeder Kompetenz sind:

- Verfügbarkeit und Bewertung von Wissen (zum Beispiel nach Brauchbarkeit und Handlungsrelevanz),
- Interpolationsfähigkeit, um Wissenslücken zu überdecken (Erfahrung, Fähigkeit zur Risikoabschätzung),
- Handlungsfähigkeit und Handlungsorientierung (Auseinandersetzung mit Umwelt, Entscheidung über Unsicherheit und bestimmungsgemäßem Handeln).

Damit wird über alle Begriffe wie „Können" und „Qualifikation" die Selbstorganisationsfähigkeit von handelnden Personen beschrieben.

4 ArbSchG 1996.
5 BAuA 2004.





Seit in den 1990er Jahren die Kompetenzdiskussion über die Berufspädagogik hinausgelangt ist (Staudt, Erpenbeck[6, 7, 8, 9, 10]), wird die Wissenschaft von einer Vielfalt an Kompetenzbegriffen überschwemmt wie unter anderem „Fach"-, „Methoden"-, „Lern"-, „Personal"-, „Führungskompetenz". Vielfach werden Gruppen gebildet, zum Beispiel die der „Schlüssel"- und „Kernkompetenzen". Während die „Schlüsselkompetenzen" auf die personelle oder individuelle Ebene fokussiert sind wie

- Individualkompetenzen (Reflexionsfähigkeit, Flexibilität, Verantwortlichkeit usw.),
- Sozialkompetenzen (Teamfähigkeit, Einfühlungsvermögen, Konfliktlösungsbereitschaft usw.),
- Methodenkompetenzen (analytisches und strukturelles Denken, Lernfähigkeit, Medienkompetenz und andere),
- Fachkompetenzen

bilden die „Kernkompetenzen" eine Verbindung zur institutionellen Ebene. Sie basieren auf dem Wissen, den Fähigkeiten und Erfahrungen der handelnden Personen in einer Organisation, die sie in einer einzigartigen Kombination von tief verwurzelten Kompetenzen zu erfolgreichen Produkten führen.



Dieses „kollektive Wissen" einer Organisation oder eines Unternehmens, welches sich in dessen Fähigkeiten äußert, bedarf einer Fülle individuellen Wissens auf den Gebieten der Technik (Herstellungstechniken, Integration unterschiedlicher Technologiebereiche), der Organisation (Projektmanagement, innerbetriebliche Kommunikation, Informationsmanagement) und deren Spiegelung durch die gesammelten Erfahrungen und das erworbene Anwendungswissen.

Nach Prahalad/Hamel[11], Kotler/Bliemel[12] und Krüger/Hamp[13]

- haben Kernkompetenzen das Potenzial für erfolgreiches Agieren auf Märkten,
- leisten Kernkompetenzen wesentliche Beiträge zum wahrgenommenen Kundennutzen,
- sichern Kernkompetenzen die Übertragbarkeit auf konkrete Produkte und Leistungen und
- sind Kernkompetenzen schwierig (nicht kurzfristig) zu kopieren.



6 ABWF/QUEM 2005.
7 Erpenbeck/Rosenstiel 2007.
8 QUEM-report 2007.
9 Risch/Israel 2005.
10 Risch 2002.
11 Prahalad/Hamel 1990.
12 Kotler/Bliemel 2001.
13 Hamp/Krüger 1997.





Für viele Produkte, zum Beispiel im Maschinenbau, stellt neben der technischen Güte und Wirksamkeit die Anlagensicherheit eine entscheidende Kernkompetenz dar. Dasselbe gilt für die technologische Sicherheit der Prozesse, angefangen bei den Endproduzenten (OEM) und endend bei einem Teilezulieferer oder einem Handwerksbetrieb.

1.4 AUSBLICK

Wissend, dass solcherart Kernkompetenzen nicht durch den Erwerb einer formalen Qualifikation (Testat, Befähigungsnachweis) allein aufgebaut werden können, bietet gerade die Beschäftigung mit dem Themenfeld Sicherheit Anlass, über das bisherige Qualifikationsdenken hinauszugehen.

Die Beschäftigung mit Kernkompetenzen kann die Sicherheitsdiskussion befruchten, weil Kernkompetenzen

- oft komplex sind und nicht durch einen einzigen Faktor, sondern eine bestimmte Kombination mehrerer Faktoren begründet sind,
- aufgrund individueller Lernprozesse zum Wissen einer Organisation führen,
- eine Marke für ein Unternehmen sein können,
- Innovativität befördern




und Sicherheit vom Kunden bzw. Nutzer zumeist vorausgesetzt, aber im wirtschaftlichen (wie auch wissenschaftlichen) Mainstream kaum thematisiert wird.

Es gilt, bei der Enthüllung von Kernkompetenzen die Diskussion auf die Ermittlung von Erklärungsmustern zu lenken und sie verstärkt auf solche zu fokussieren, die das Thema „Sicherheit" explizit tangieren oder vielleicht in jüngster Vergangenheit in den Hintergrund haben treten lassen.

1.5 LITERATUR

ABWF/QUEM 2005
ABWF/QUEM: Kompetenzmessung im Unternehmen, Münster/ New York, Waxmann, 2005.

ArbSchG 1996
Arbeitsschutzgesetz vom 7. August 1996 (BGBl. I S. 1246), zuletzt geändert durch Art. 15 Abs. 89 des Gesetzes vom 5. Februar 2009 (BGBl. I S. 160).





BAuA 2004
Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (Hrsg.): Ratgeber zur Ermittlung gefährdungsbezogener Arbeiztschutzmaßnahmen im Betrieb – Handbuch für Arbeitsschutzfachleute, 4. Aufl. Dortmund, Berlin 2004. URL: http://www.baua.de/de/Themen-von-A-Z/Gefaehrdungsbeurteilung/pdf/Ratgeber-Gefaehrdungsbeurteilung.pdf [Stand: 22.07.2009].

DIN 1987
DIN Deutsches Institut für Normung e. V.: DIN VDE 31000 Teil 2 Allgemeine Leitsätze für das sicherheitsgerechte Gestalten technischer Erzeugnisse – Begriffe der Sicherheitstechnik – Grundbegriffe, Dez. 1987 (zurückgezogen).

DIN 2008
DIN Deutsches Institut für Normung e. V.: DIN 820-120: Normungsarbeit - Teil 120: Leitfaden für die Aufnahme von Sicherheitsaspekten in Normen, (ISO/IEC Guide 51:1999), Berlin: Beuth, 2008.

Erpenbeck/Rosenstiel 2007
Erpenbeck, John/von Rosenstiel, Lutz (Hrsg.): Handbuch Kompetenzmessung, Stuttgart: Schäffer-Poeschel, 2007.



Hamp/Krüger 1997
Hamp, C./Krüger, W.: Kernkompetenz-Management, Gabler, 1997.

Kotler/Bliemel 2001
Kotler, P./Bliemel, F.: Marketing-Management, Schäffer-Poeschel, Stuttgart, 2001.

Maslow 1943
Maslow, Abraham: „A Theory of Human Motivation“. In: Psychological Review 50 (1943), S. 370-396.

Pralahad/Hamel 1990
Prahalad, C.K./Hamel, G.: „The Core Competence of the Corporation.” In: Harvard Business Review May/June 1990.

QUEM-report 2007
Arbeitsgemeinschaft Betriebliche Weiterbildungsforschung e. V. (Hrsg.): Projektübergreifende Evaluation von Gestaltungsprojekten im Programmbereich „Lernen im Prozess der Arbeit“, QUEM-report, Heft 99, Berlin, 2007.



Risch 2002
Risch, W. (Hrsg.): Arbeit im E-Business – Personal und Einführungsprozess, Chemnitz: ATB-Eigenverlag, 2002.

Risch/Isreal 2005
Risch, W./Israel, D.: „Prozessbegleitende Lernformen als Antwort auf den Wandel der Kompetenzanforderungen in der Wirtschaft." In: Albrecht, G./Bähr, W. H. (Hrsg.): Berufsbildung im Wandel, Berlin/Bonn: IFA-Verlag, 2005.








2 VERZAHNUNG VON AUS- UND WEITERBILDUNG – DIE LÖSUNG FÜR SICH STÄNDIG ÄNDERNDE ANFORDERUNGEN?

WOLFRAM RISCH

2.1 EINFÜHRUNG

Die Vorbetrachtungen von Pfeil/Risch machen deutlich, dass Sicherheit eine Kernkompetenz für die Wettbewerbsfähigkeit und die Nachhaltigkeit für Unternehmen und die Gesellschaft ist. Bei ersten Untersuchungen zur Verzahnung von Aus- und Weiterbildung auf dem Gebiet der Sicherheit[1] konnte der Widerspruch zwischen dem Erkennen der Bedeutung von sicherheitsrelevantem Wissen und dem fehlenden Aufbau eines effizienten Aus- und Weiterbildungsmanagements inklusive erforderlicher Forschungsanteile bestätigt werden.

Daher nehmen Unternehmen eine externe Unterstützung in Form von punktuellen Qualifizierungen oder Beratungen in Anspruch, allerdings oft ohne ausreichende Konzepte hinsichtlich des langfristigen Aufbaus von Kompetenzen bzw. Kernkompetenzen. Ein neuer Zugang eröffnet sich offenbar aus der Untersuchung der Verzahnung aller in Unternehmen stattfindenden Lernprozesse, zum Beispiel bei der Entwicklung der Sicherheitsfähigkeit von Organisationen. Für die Kompetenzentwicklung der Mitarbeiter sind in erster Linie beruflich-betriebliche Bildungsprozesse verantwortlich. Diese lassen sich optimieren, wenn Aus- und Weiterbildung in engem Zusammenhang mit den betrieblichen Prozessen (Innovationsprozessen, technologischen Abläufen, Arbeitsorganisation etc.) und den angestrebten Zielen (unter anderem Rendite, Umsatz, Produkt- und Prozesssicherheit) betrachtet und realisiert wird. Es geht dabei nicht um eine lineare Verbindung in einem Vieleck zwischen den einzelnen Elementen Aus- und Weiterbildung, Arbeitsprozess, Innovationsprozess, Sicherheit usw. Vielmehr geht es um eine Verzahnung von Lernen und Arbeiten zu einem einheitlichen Prozess der beruflichen Kompetenzentwicklung in Unternehmen und Organisationen.

[1] Risch 2008.



Die gegenwärtige Diskussion wird unter anderem geprägt durch:

- einerseits Reduzierung des Menschen als Sicherheitsrisiko (Faktor Mensch, Fehler, Toleranz) im Kontext zur Vertrauensbildung; andererseits werden Bildung und Kompetenz als Voraussetzungen für Sicherheit schaffende Strukturen gesehen;[2]
- schwerpunkthafte Setzung der Sicherheitsforschung auf Informationssicherheit, Überwachung und Identifikation, Schutzsysteme, Risikoanalysen, Technologiestudien, Monitoring von Gefahrstoffen usw.[3]
- die Existenz unterschiedlicher begrifflicher Auffassungen zum Themenfeld „Sicherheit", eine Vielzahl sicherheitsmethodischer Vorgehensweisen und dadurch, dass sicherheitsrelevantes Fach- und Methodenwissen kaum noch Bestandteil der universitären Ingenieurausbildung ist;[4]
- erste Erfahrungen bei der Umsetzung der neuen Luftsicherheits-Schulungsverordnung[5], die Einzelheiten der Schulung (Grundausbildung), Zusatzschulung (Erweiterung der Befähigung) und Weiterbildung (Kenntniserhalt, -auffrischung, -erweiterung) für den Personalkreis Luftsicherheitskontrollkräfte (Personal-, Waren- und Frachtkontrolle), Sicherheitspersonal, Ausbildungspersonal regelt. Trotz des scheinbar klar strukturierten und durchgängigen Regelwerkes erweist sich die Umsetzung in der Praxis für Sicherheitsdienste und Kunden als problembehaftet.[6]

Bei der Fülle der Probleme im Themenfeld Sicherheit sieht sich der Autor natürlich mit der Frage konfrontiert:

Was bedeutet Verzahnung in der Aus- und Weiterbildung mit Bezug zur Sicherheitsthematik?

Die Verbindung von Ausbildung, Weiterbildung und schöpferischen Gestaltungsprozessen gehört zu den ältesten Formen des Lernens. Erst der hohe Grad von Arbeitsteilung und damit verbundener beruflicher Spezialisierung über längere Zeiträume haben zur teilweisen (organisatorischen) Trennung von Aus- und Weiterbildung, schöpferischen und Routineprozessen geführt. Moderne Formen der Kompetenzentwicklung entstehen häufig aus der Kombination früherer Lösungsansätze, gepaart mit Methoden und Werkzeugen heutiger Medien.

Es ist anzunehmen, dass erworbene Kernkompetenzen eine höhere Langzeitwirkung und Beständigkeit gegenüber raschen und teilweise nicht vorhersehbaren Risiken, Unfällen oder Katastrophen haben als kurzfristig erworbene Qualifikationen. Die Aneignung

2 Österreichische Akademie der Wissenschaften 2005.
3 Thoma 2008.
4 Vgl. der Beitrag von Beyerer et al. in diesem Band.
5 LuftSiSchulV 2008.
6 Wermann et al. 2009; SECURITAS – Luftsicherheits-Schulungsverordnung; Praktische Auswirkungen auf Sicherheitsunternehmen.





von Methoden und Verfahren typischer sicherheitsrelevanter Problemlösungsprozesse und die Ausprägung von Grundlagen für die Fähigkeit arbeitsbegleitenden Lernens sind Aspekte, die als besonders wichtig für eine nachhaltige Wirkung sicherheitsadäquaten Handelns angesehen werden.

Die Arbeitsplätze in der Sicherheitswirtschaft beispielsweise zeichnen sich aus durch:

- stärker kompetenzgeprägte und weniger qualifikationsbezogene Arbeitsanforderungen, auch wenn der Zugang zumeist noch über Befähigungsnachweise und Kurzlehrgänge erfolgt, sowie
- ein erfahrungs- und tätigkeitsbegleitendes Neu- und Weiterlernen.

Das traditionelle Verständnis von einer Erstausbildung, welches im Sicherheitsgewerbe nur als Fachkraft für Schutz und Sicherheit existiert und dem nachfolgenden Erwerb von Zusatzqualifikationen für den Arbeitsplatz dient, trifft nicht zu. Vielmehr rekrutieren sich die mit dem Thema „Sicherheit" befassten (oder teilweise befassten) Beschäftigten aus unterschiedlichen Berufen und Tätigkeiten.





Anzustrebende Ziele der Verzahnung von prozessintegrierter beruflicher Ausbildung und betrieblicher (beruflicher) Weiterbildung auf dem Gebiet der Sicherheit resultieren aus:

- dem Bestreben der Aneignung der beruflichen Handlungskompetenz für sicherheitstangierende Arbeitsaufgaben einer vergleichbaren Problemklasse, wo das Lernen dem Erwerb von Fach- und Methodenkompetenz dient;
- der Notwendigkeit zur Befähigung zum erfahrungsgeleiteten und fremdinduzierten Lernen, wo dies zu einer allgemeinen Lernkompetenz führt;
- der Notwendigkeit, in disziplinübergreifenden leistungsfähigen und leistungsbereiten Teams mitzuwirken, wo das Lernen der Entwicklung von Sozialkompetenz dient.

Die Verzahnung gelingt nur erfolgreich, wenn sie auf die arbeitsprozessbezogene Aneignung von beruflichen – in diesem Fall sicherheitsbezogenen – Kompetenzen und zugleich auf Verhaltensänderungen des Mitarbeiters als Arbeitenden und Lernenden gerichtet ist. Dadurch gilt es, traditionelle Widersprüche zwischen Lern- und Arbeitsprozess sowie zwischen Aus- und Weiterbildung schrittweise zu lösen.





2.2 KURZRECHERCHE ZUM THEMA SICHERHEIT IN DER AUS- UND WEITERBILDUNG[7]

Folgende Fragestellungen standen im Zentrum der Recherche:

- Was wird angeboten?
- Was sind die Hauptinhalte?
- Wer bietet es an?
- Wo wird es angeboten?
- Wie wird es genutzt (je nach Datenlage)?
- „Wie viel Sicherheit" ist in anderen enthalten?

Eingangsfeststellungen:

a) Die Suche in Anbieterportalen von Bildungsdienstleistern ergab zwar Treffer für „Sicherheit", aber keine für „Security" und für „Safety".
b) „Safety" und „Security" werden im Bildungsbereich bis hin zu den Inhalten nicht in dieser Art differenziert.
c) Im akademischen Bildungsbereich trifft man vereinzelt auf Differenzierungen nach „Safety" und „Security".
d) Im deutschen Sprachgebrauch bezieht sich „Security" hauptsächlich auf Personenschutz.
e) Es gibt nur einen anerkannten Ausbildungsberuf bzw. Berufsabschluss im Bereich Sicherheit. Alles andere sind (Weiter-)Bildungsmodule.

2.2.1 AUSBILDUNG

2.2.1.1 FACHKRAFT FÜR SCHUTZ UND SICHERHEIT[8]

Fachkräfte für Schutz und Sicherheit unterstützen die öffentliche, private und betriebliche Sicherheit und Ordnung. Sie schützen Personen, Sachwerte und immaterielle Werte, insbesondere durch präventive Maßnahmen und, soweit erforderlich, durch Gefahrenabwehr.

7 Risch/Raßbach 2008.
8 Vgl. Bundesgesetzblatt 2008.







Sie arbeiten in Unternehmen der Sicherheitsbranche sowie in verschiedenen Bereichen der Unternehmenssicherheit, des öffentlichen Dienstes und der Verkehrswirtschaft.

Die Fachkraft für Schutz und Sicherheit wird dem Ausbildungsbereich Industrie und Handel zugeordnet. Die dreijährige Ausbildung findet an den Lernorten Betrieb und Berufsschule statt.

Fachkräfte für Schutz und Sicherheit haben folgende berufliche Qualifikationen:

- Sie planen und führen Maßnahmen der Sicherung und präventiven Gefahrenabwehr durch;
- sie analysieren Gefährdungspotenziale, entwickeln Sicherungsmaßnahmen und leiten diese ein;
- sie überprüfen und überwachen die Einhaltung objektbezogener Schutz- und Sicherheitsvorschriften, insbesondere zum Arbeitsschutz, Brandschutz, Umweltschutz und Datenschutz;
- sie beobachten die Branchenentwicklung und bewerten die Auswirkungen auf das betriebliche Leistungsangebot;
- sie wirken bei der Angebotserstellung und Auftragsbearbeitung mit;
- sie ermitteln, klären auf und dokumentieren sicherheitsrelevante Sachverhalte;
- sie überprüfen die ordnungsgemäße Funktion von Schutz- und Sicherheitseinrichtungen und leiten bei Mängeln Maßnahmen ein;
- sie identifizieren Wirkungsweise und Gefährdungspotenzial von Waffen, gefährlichen Gegenständen und Stoffen;
- sie sind in der Lage, bei Schutz- und Sicherheitsmaßnahmen sich situations- und personenbezogen zu verhalten und entsprechend zu handeln;
- sie arbeiten selbstständig, team- und kundenorientiert sowie in Kooperation mit anderen Dienstleistungsbereichen.








Abbildung 1: Daten zur Nutzung der Ausbildung „Fachkraft für Schutz und Sicherheit“[9]

	DEUTSCHLAND			SACHSEN			BW**	BAYERN
	2004	2005	2006	2004	2005	2006	2006	2006
Neuabschlüsse	759	714	972	62	34	57	99	147
Auszubildende	1282	1695	2110	102	113	132	175	341
Regionaler Anteil in %			100			6,3	16,2	8,3
Frauenanteil in %	19,0	19,5	20,3	14,7	14,2	18,2	26,3	22,6
Ausländeranteil	5,2	5,0	4,4	0,0	0,9	0,8	8,6	7,6
Prüfungsteilnehmer	9	332	832	0	14	60	39	90
Erfolgsquote in %*	33,3	78,5	68,7		100	40,7	79,4	76,3
Anzahl Ausbildungsstätten³*			513			k. A.	k. A	k. A.
Auszubildende pro Ausbildungsstätte³*			4,1			k A.	k. A.	k. A.

* unter Berücksichtigung der Wiederholer, ** Baden-Württemberg, ³* Quelle DIHK




2.2.1.2 SERVICEKRAFT FÜR SCHUTZ UND SICHERHEIT[10]

Servicekräfte für Schutz und Sicherheit unterstützen die öffentliche, private und betriebliche Sicherheit und Ordnung. Sie schützen Personen, Sachwerte und immaterielle Werte, insbesondere durch Umsetzung präventiver Maßnahmen und, soweit erforderlich, durch Gefahrenabwehr.

Sie arbeiten in Unternehmen der Sicherheitsbranche sowie in verschiedenen Bereichen der Unternehmenssicherheit, des öffentlichen Dienstes und der Verkehrswirtschaft.

Die Servicekraft für Schutz und Sicherheit wird dem Ausbildungsbereich Industrie und Handel zugeordnet. Die zweijährige Ausbildung findet an den Lernorten Betrieb und Berufsschule statt.

[9] BIBB 2008: Datenblätter der Datenbank Aus- und Weiterbildungsstatistik des Bundesinstituts für Berufsbildung (BIBB) auf Basis der Berufsbildungsstatistik des Statistischen Bundesamtes (StBA) (Erhebung zum 31. Dezember) , Internet: http://www.bibb.de/de/781.htm (Zugriff: 07.10.2008).

[10] Nachfolgendes gilt erst seit 2008 mit der Verordnung über die Berufsausbildung zur Servicekraft für Schutz und Sicherheit vom 21.05.2008, BGBl I, Nr. 21, S. 940.



Servicekräfte für Schutz und Sicherheit haben folgende berufliche Qualifikationen:

- sie führen Maßnahmen der Sicherung und präventiven Gefahrenabwehr durch;
- sie beurteilen Gefährdungspotenziale und leiten Sicherungsmaßnahmen ein;
- sie überprüfen und überwachen die Einhaltung objektbezogener Schutz- und Sicherheitsvorschriften, insbesondere zum Arbeitsschutz, Brandschutz, Umweltschutz und Datenschutz;
- sie wirken bei der Ermittlung und Aufklärung von sicherheitsrelevanten Sachverhalten mit und dokumentieren diese;
- sie überprüfen die ordnungsgemäße Funktion von Schutz- und Sicherheitseinrichtungen und leiten bei Mängeln Maßnahmen ein;
- sie identifizieren Wirkungsweise und Gefährdungspotenzial von Waffen, gefährlichen Gegenständen und Stoffen;
- sie sind in der Lage, bei Schutz- und Sicherheitsmaßnahmen sich situations- und personenbezogen zu verhalten und entsprechend zu handeln;
- sie arbeiten team- und kundenorientiert sowie in Kooperation mit anderen Dienstleistungsbereichen.





2.2.2 BERUFSBEZOGENE FORT- UND WEITERBILDUNG

2.2.2.1 GEPRÜFTER MEISTER/GEPRÜFTE MEISTERIN FÜR SCHUTZ UND SICHERHEIT

Geprüfte Meister und geprüfte Meisterinnen für Schutz und Sicherheit sind befähigt, in privaten und öffentlichen Unternehmen unterschiedlicher Größe und Branchenzugehörigkeit sowie in verschiedenen Bereichen und Tätigkeitsfeldern eines Unternehmens Sach-, Organisations- und Führungsaufgaben wahrzunehmen und sich auf veränderte Methoden und Systeme, auf sich verändernde Strukturen der Arbeitsorganisation und auf neue Methoden der Organisationsentwicklung, der Personalführung und -entwicklung flexibel einzustellen sowie den technisch-organisatorischen Wandel im Unternehmen mitzugestalten.



Sie sind befähigt und befugt, Aufgaben der betrieblichen Aus- und Weiterbildung wahrzunehmen (Ausbilderkompetenz).

Daten:[11]

- Die Prüfung wurde 2006 bundesweit von 109 Personen (davon 3 Frauen) angetreten und mit einer Erfolgsquote von 74 Prozent absolviert.
- Nach Bundesländern unterschieden, sind in Baden-Württemberg 14, in Berlin 13, in Brandenburg 12, in Hamburg 56, in Mecklenburg-Vorpommern 4 und Thüringen 29 Personen zur Prüfung angetreten.

2.2.2.2 SCHUTZ- UND SICHERHEITSFACHKRAFT (GEPRÜFT IHK)

Mit Abschluss dieser Fortbildungsprüfung soll festgestellt werden, ob die Qualifikation besteht, Aufgaben in der Sicherheitswirtschaft (gewerbliche Sicherheitsunternehmen und betriebliche Sicherheitseinrichtungen) insbesondere in Bewachungs-, Sicherungs- und Ordnungsdiensten, Veranstaltungs- und Verkehrsdiensten wahrzunehmen. Die Prüfung stellt die „Ersatz"-Qualifikation für Seiteneinsteiger nach dem Wegfall der geprüften Werkschutzfachkraft dar.

Drei Handlungsbereiche werden genannt:

- rechts- und aufgabenbezogenes Handeln,
- Gefahrenabwehr sowie Einsatz von Schutz- und Sicherheitstechnik,
- sicherheits- und serviceorientiertes Verhalten und Handeln.

Voraussetzungen für die Zulassung zur Prüfung sind:

- eine mit Erfolg abgeschlossene Ausbildung in einem anerkannten Ausbildungsberuf und eine weitere einschlägige Berufspraxis von mindestens zwei Jahren in der Sicherheitswirtschaft
- oder eine mindestens fünfjährige Berufspraxis, von der mindestens drei Jahre in der Sicherheitswirtschaft abgeleistet sein müssen,
- ein Mindestalter von 24 Jahren und
- die Teilnahme an einem Erste-Hilfe-Lehrgang, dessen Beendigung nicht länger als 24 Monate zurückliegt.

[11] BIBB 2008: Datenblätter der Datenbank Aus- und Weiterbildungsstatistik des Bundesinstituts für Berufsbildung (BIBB) auf Basis der Berufsbildungsstatistik des Statistischen Bundesamtes (StBA) (Erhebung zum 31. Dezember) , Internet: http://www.bibb.de/de/781.htm (Zugriff: 07.10.2008).







Daten:[12]

- Die Prüfung wurde 2006 bundesweit von 183 Personen (davon 25 Frauen) mit einer Erfolgsquote von 71,6 Prozent angetreten.
- Nach Bundesländern unterschieden, sind in Baden-Württemberg 45, in Berlin 39, in Hessen 10, in Niedersachsen 22, in Schleswig-Holstein 12, in Mecklenburg-Vorpommern 5, in Nordrhein-Westfalen 6, im Saarland 11, in Sachsen-Anhalt 12 und Thüringen 21 Personen zur Prüfung angetreten.

2.2.2.3 FACHKRÄFTE FÜR SPEZIELLE TÄTIGKEITSBEREICHE

2.2.2.3.1 FACHKRAFT UMWELTSCHUTZ

Die Tätigkeit im Überblick: Fachkräfte für Umweltschutz beraten und begleiten Betriebe in Umweltfragen und sorgen für die Umsetzung von Umweltschutzbedingungen.

Fachkräfte für Umweltschutz sind in Unternehmen der unterschiedlichsten Wirtschaftsbereiche mit Aufgaben des betrieblichen Umweltschutzes oder der Einführung von umweltfreundlichen Produktionsmethoden befasst. Ebenso können sie bei Beratungsunternehmen und -institutionen beschäftigt sein.

Die Ausbildung im Überblick: „Fachkraft für Umweltschutz" ist eine Weiterbildung, die durch interne Vorschriften der Bildungsanbieter geregelt ist.

Die Lehrgänge werden von privaten Bildungsinstituten sowie an Bildungseinrichtungen der Industrie- und Handelskammern und Handwerkskammern durchgeführt. Die Lehrgänge werden im Vollzeit- und Teilzeitunterricht angeboten und sind in ihrer Dauer sehr unterschiedlich. Eine berufsbegleitende Weiterbildung dauert als Grundstufenlehrgang 15 Wochen. Als Wochenendveranstaltung finden Lehrgänge mit einer Dauer von knapp einem halben Jahr statt.

Für die Fachkraft für Umweltschutz können die drei Schwerpunkte gewählt werden:

- Fachkraft für Umweltschutz Schwerpunkt Abfallwirtschaft
- Fachkraft für Umweltschutz Schwerpunkt Gewässerschutz
- Fachkraft für Umweltschutz Schwerpunkt Immissionsschutz

[12] BIBB 2008: Datenblätter der Datenbank Aus- und Weiterbildungsstatistik des Bundesinstituts für Berufsbildung (BIBB) auf Basis der Berufsbildungsstatistik des Statistischen Bundesamtes (StBA) (Erhebung zum 31. Dezember) , Internet: http://www.bibb.de/de/781.htm (Zugriff: 07.10.2008).





2.2.2.3.2 FACHKRAFT BRANDSCHUTZ

Die Tätigkeit im Überblick: Brandschutzfachkräfte kümmern sich um Maßnahmen zur Brand- und Explosionsbekämpfung. Frühzeitige Gefahrenerkennung und Vorbeugung gehören ebenso zu ihren Aufgaben wie Schulungen für das Verhalten im Ernstfall.

Brandschutzfachkräfte arbeiten in erster Linie in Betrieben, in denen erhöhte Brandgefahr besteht wie beispielsweise bei Flughafenbetrieben, in der Metall- oder Chemieindustrie sowie in Kraftwerken. Auch in Lackfabriken, Kunststofffabriken, bei Herstellern von pharmazeutischen Stoffen oder im Bergbau finden sie Beschäftigungsmöglichkeiten.

Die Ausbildung im Überblick: „Brandschutzfachkraft" ist eine durch interne Regelungen oder durch Industrie- und Handelskammern geregelte berufliche Weiterbildung.

Die Lehrgänge unterschiedlicher Dauer werden an Bildungseinrichtungen verschiedener Träger (zum Beispiel TÜV-Akademien, Umweltinstituten oder Bildungszentren der Industrie- und Handelskammern) durchgeführt. Es können folgende Schwerpunkte gewählt werden:



- Fachplaner für vorbeugenden Brandschutz
- Sachverständiger für vorbeugenden Brandschutz
- Fachplaner für gebäudetechnischen Brandschutz
- Sachverständiger für brandschutztechnische Bau- und Objektüberwachung



2.2.2.3.3 FACHKRAFT ARBEITSSICHERHEIT

Die Tätigkeit im Überblick: Fachkräfte für Arbeitssicherheit beraten und unterstützen den Arbeitgeber und die zuständigen Führungskräfte beim Arbeitsschutz und bei der Unfallverhütung in allen Fragen der Arbeitssicherheit einschließlich der ergonomischen Gestaltung der Arbeit und Arbeitsplätze.

Fachkräfte für Arbeitssicherheit arbeiten überwiegend in Produktionsbetrieben. Das können Industrie- oder Handwerksbetriebe nahezu aller Wirtschaftszweige sein. Aber auch in Handels- oder Dienstleistungsunternehmen sowie in Verwaltungseinrichtungen können sie beschäftigt sein.

Die Ausbildung im Überblick: „Fachkraft für Arbeitssicherheit" ist eine Weiterbildung, die auf Grundlage der von der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA) und dem Hauptverband der gewerblichen Berufsgenossenschaften (HVBG) erarbeiteten Richtlinien durchgeführt wird.Die Weiterbildung wird von staatlichen und berufsgenossenschaftlichen Bildungseinrichtungen oder von staatlich bzw. berufsgenossenschaftlich anerkannten Lehrgangsträgern durchgeführt und dauert je nach Art der Lehrgänge und Bildungsanbieter zwölf Wochen bis drei Jahre.





2.2.2.3.4 FACHKRAFT STRAHLENSCHUTZ

Die Tätigkeit im Überblick: Aufgabe von Strahlenschutzfachkräften ist es, Menschen, Gesundheit und Sachgüter vor dem Einwirken schädlicher ionisierender Strahlen zu schützen. In Kliniken und in Unternehmen mit kerntechnischen Anlagen entwickeln sie Schutzmaßnahmen, beraten Mitarbeiter/innen und Führungskräfte und führen regelmäßig Messungen durch.

Strahlenschutzfachkräfte arbeiten zum Beispiel in Kliniken mit radiologischen Abteilungen oder in Unternehmen mit kerntechnischen Anlagen wie Atomkraftwerken sowie in kerntechnischen Forschungseinrichtungen. Auch Herstellerfirmen für nukleartechnischen Anlagenbau oder spezialisierte Entsorgungsbetriebe kommen als Arbeitgeber infrage. Darüber hinaus sind geeignete Tätigkeitsfelder in Forschungsbereichen von Hochschulen oder auch in Ingenieurbüros und bei Gewerbeaufsichtsämtern denkbar.

Die Ausbildung im Überblick: „Strahlenschutzfachkraft" ist eine durch die Industrie- und Handelskammer Aachen geregelte berufliche Weiterbildung nach dem Berufsbildungsgesetz (BBiG).



Die Dauer der Vorbereitungskurse für die Prüfung beträgt in Vollzeit drei bis vier Monate. Bei Teilzeitlehrgängen wird die Kursdauer wesentlich von der Art der Teilzeitmaßnahme (zum Beispiel mit oder ohne Wochenendveranstaltungen) sowie vom Umfang des wöchentlichen Unterrichtsangebots bestimmt. Im Regelfall dauern die Vorbereitungskurse in Teilzeitform etwa sechs Monate.

2.2.2.3.5 IT-SICHERHEITSKOORDINATOR/IN

Die Tätigkeit im Überblick: IT-Sicherheitskoordinatoren und -koordinatorinnen konzipieren angemessene IT-Sicherheitslösungen entsprechend den geltenden technischen Standards, Gesetzen und Vorschriften. Sie begleiten deren Umsetzung und passen sie laufend den aktuellen Gegebenheiten an.

IT-Sicherheitskoordinatoren und -koordinatorinnen arbeiten in Firmen der IT-Branche. Darüber hinaus können sie in Handwerks- oder Industrie- und Handelsbetrieben der unterschiedlichsten Wirtschaftszweige beschäftigt sein. Ebenso sind sie im Dienstleistungsbereich oder in der öffentlichen Verwaltung tätig.

Die Ausbildung im Überblick: „IT-Sicherheitskoordinator/in" ist eine Weiterbildung in Form eines Selbststudiums, die mit einem Zertifizierungsverfahren abschließt.

Die Industrie- und Handelskammern bieten Zertifizierungen zum IT Security Coordinator (IHK) an. Vorbereitungskurse hierzu finden in der Regel in Teilzeit statt.





Im Rahmen eines vom Bundesministerium für Bildung und Forschung initiierten und geförderten Großprojektes zum Aufbau eines modernen IT-Weiterbildungssystems wurde dieses in drei aufeinander aufbauende Ebenen (Karrierestufen) gegliedert: Spezialisten, operative und strategische Professionals. IT-Sicherheitskoordinator/in gehört zur unteren Ebene, den Spezialisten.

Die Dauer der Weiterbildung ist nicht vorgeschrieben und kann daher unterschiedlich sein. Sie liegt erfahrungsgemäß bei ca. einem Jahr.

2.2.2.4 BEAUFTRAGTE

Beauftragte sind zwar im Regelfall Personen mit Hochschulabschluss, doch der Zugang ist ebenfalls als Facharbeiter möglich.

2.2.2.4.1 GEWÄSSERSCHUTZBEAUFTRAGTE/R (ALS SPEZIALISIERUNG/FUNKTION)

Die Tätigkeit im Überblick: Gewässerschutzbeauftragte kontrollieren und überwachen die Abwasseranlagen und stellen sicher, dass die Vorschriften und Auflagen des Gewässerschutzes eingehalten werden.



Gewässerschutzbeauftragte arbeiten in erster Linie in Betrieben der Ver- und Entsorgung, zum Beispiel bei Gasversorgern, Betreibern von Kläranlagen oder in Recyclingunternehmen. Auch bei Umweltämtern sowie in Ingenieurbüros für Umwelttechnik, Abfalltechnik und Entsorgung sind sie tätig. Die chemische Untersuchung und Beratung bietet weitere Beschäftigungsmöglichkeiten.

Zugang: Um diese Tätigkeit ausüben zu können, wird üblicherweise eine Weiterbildung in der Umweltschutztechnik oder ein Hochschulstudium, zum Beispiel der Naturwissenschaften oder der Umweltökonomie, gefordert. Außerdem ist ein Nachweis über die notwendige Fach- und Sachkenntnis erforderlich.

2.2.2.4.2 IMMISSIONSSCHUTZBEAUFTRAGTE/R (ALS SPEZIALISIERUNG/FUNKTION)

Die Tätigkeit im Überblick: Immissionsschutzbeauftragte beraten Anlagenbetreiber bzw. Beauftragte, wie etwa Werkleiter/innen, in allen für den Immissionsschutz bedeutsamen Fragen unter Berücksichtigung der jeweiligen betrieblichen Gegebenheiten. Sie sind auch Ansprechpartner für die Überwachungsbehörden.

Immissionsschutzbeauftragte arbeiten in erster Linie in Betrieben der Ver- und Entsorgung, zum Beispiel bei Gaserzeugern und Recyclingunternehmen. Auch bei Umweltämtern sowie in Ingenieurbüros für Umwelttechnik, Abfalltechnik und Entsorgung sind sie tätig. Die chemische Untersuchung und Beratung bietet weitere Beschäftigungsmöglichkeiten.

Zugang: Um diese Tätigkeit ausüben zu können, wird üblicherweise ein Hochschulstudium im Bereich Ingenieurwesen, Chemie oder Physik gefordert. Außerdem müssen angehende Immissionsschutzbeauftragte an von der zuständigen Behörde anerkannten





Lehrgängen teilnehmen, in denen fachkundliche Kenntnisse vermittelt werden. Darüber hinaus wird eine zweijährige praktische Tätigkeit gefordert, die auf ihre künftigen Aufgaben vorbereitet.

Außerdem kann gegebenenfalls auch eine technische Fachschulausbildung oder die Qualifikation als Meister Zugang zur Tätigkeit gewähren. Dies setzt unter anderem eine mindestens vierjährige praktische Tätigkeit voraus.

Geregelt ist dies in der Verordnung zur Durchführung des Immissionsschutz-Gesetzes.

2.2.2.4.3 STRAHLENSCHUTZBEAUFTRAGTE/R (ALS SPEZIALISIERUNG/FUNKTION)

Die Tätigkeit im Überblick: Strahlenschutzbeauftragte kümmern sich darum, dass in Betrieben die Strahlenschutzgrundsätze und erlassene behördliche Anordnungen eingehalten werden.

Strahlenschutzbeauftragte arbeiten in erster Linie in Kernkraftwerken sowie in der Wiederaufbereitung oder Beseitigung nuklearer Abfälle, in Krankenhäusern oder in Unternehmen der chemischen Industrie. Auch bei Umweltämtern und Strahlenschutzbehörden sind sie tätig. Technische Überwachungsvereine bieten weitere Beschäftigungsmöglichkeiten.



Zugang: Um diese Tätigkeit ausüben zu können, ist üblicherweise eine Weiterbildung in der Umweltschutztechnik oder im Strahlenschutz bzw. ein ingenieur- oder betriebswirtschaftliches Hochschulstudium mit entsprechender Schwerpunktsetzung erforderlich. Außerdem muss ein Fachkundenachweis gemäß Strahlenschutzverordnung bzw. Röntgenverordnung erbracht werden.

2.2.2.4.4 GEFAHRGUTBEAUFTRAGTE/R (ALS SPEZIALISIERUNG/FUNKTION)

Die Tätigkeit im Überblick: Gefahrgutbeauftragte überwachen die Einhaltung der gesetzlichen Bestimmungen beim Transport gefährlicher Güter wie Gase, Gifte, Säuren oder Mineralölprodukte.

Gefahrgutbeauftragte arbeiten in erster Linie bei Transport- oder Speditionsunternehmen. Darüber hinaus sind sie in Unternehmen unterschiedlicher Wirtschaftszweige im Gefahrguttransport tätig, zum Beispiel in Betrieben der chemischen Industrie.

Zugang: Um diese Tätigkeit ausüben zu können, ist üblicherweise eine Aus- oder Weiterbildung im Verkehrs- bzw. Speditionswesen erforderlich.

Gefahrgutbeauftragte müssen einen gültigen Schulungsnachweis gemäß Gefahrgutbeauftragtenverordnung besitzen.





2.2.2.4.5 DATENSCHUTZBEAUFTRAGTE/R (ALS SPEZIALISIERUNG/FUNKTION)

Die Tätigkeit im Überblick: Datenschutzbeauftragte kontrollieren die Einhaltung der Datenschutzbestimmungen. Sie arbeiten auf ihrem Gebiet weisungsfrei und verpflichten die mit der Datenverarbeitung beauftragten Mitarbeiter auf das Datengeheimnis. Betriebe und Behörden, die personenbezogene Daten für eigene oder Geschäftszwecke elektronisch verarbeiten, zum Beispiel in der Personalabteilung oder im Rechenzentrum, müssen nach dem Bundesdatenschutzgesetz Datenschutzbeauftragte schriftlich bestellen. Datenschutzbeauftragte können in Unternehmen aller Wirtschaftszweige arbeiten, in denen personenbezogene Daten verarbeitet werden.

Das Bundesdatenschutzgesetz (BDSG) schreibt für alle Unternehmen die Bestellung eines betrieblichen Datenschutzbeauftragten vor, wenn mehr als neun Personen (inklusive Teilzeitkräfte und Leiharbeitnehmer) personenbezogene Daten automatisiert verarbeiten. Jede/r Unternehmer/in oder Geschäftsführer/in – ob mit oder ohne Datenschutzbeauftragten – sollte über die wichtigsten Forderungen des Bundesdatenschutzgesetzes informiert sein.

Zugang: Um diese Tätigkeit ausüben zu können, wird der Nachweis der erforderlichen Fachkunde sowie Zuverlässigkeit nach dem Bundesdatenschutzgesetz verlangt. Auch ein Studium in den Bereichen Rechtswissenschaften oder Informatik bzw. eine Aus- oder Weiterbildung im Bereich Datenverarbeitung/Informatik kann den Zugang ermöglichen.



2.2.2.4.6 WEITERE BEAUFTRAGTE

Ferner gibt es unter anderem noch Beauftragte auf den Gebieten der allgemeinen Sicherheit, des Laserschutzes, für Störfälle, für Abfall, für Brandschutz.

Besonders bei den Beauftragten ist die enge Verzahnung von Ausbildung/Studium und permanenter, oft spezifischer Weiterbildung eine dringliche Voraussetzung.

2.2.2.5 ALLGEMEINE WEITERBILDUNG BZW. (FACHKUNDE-) LEHRGÄNGE

Die folgende Liste stellt Beispiele von allgemeinen Weiterbildungen zum Thema „Sicherheit" vor. Sie ist jedoch nicht vollständig. Hierzu zählen die Bereiche:

- Sicherheits- und Gesundheitsschutzkoordinator/in – Aufbaulehrgang,
- CE-Kennzeichnung – Grundlagen: der einfache Weg zu EG-Konformität,
- Datenschutz und Datensicherheit in medizinischen Einrichtungen,
- Sicherheit im Handel (IHK),
- Arbeitsschutz/Baustellensicherheit – Änderungen im Vorschriftenwerk,





- Sicherheit im e-Business,
- IT- Sicherheitskompetenz,
- Bildungsangebote der ZVEI Akademie:
  - Safety (DIN 14675, VDE 0833, Brandmeldeanlagen, Fluchtsysteme),
  - Security (Blitzschutz, Einbruchmeldeanlagen).

2.2.2.6 STUDIENGÄNGE SICHERHEITSMANAGEMENT

Der Studiengang „Sicherheitsmanagement (B.A.)" der FHVD Schleswig-Holstein (zweiter Jahrgang) und der für 2010 geplante Studiengang „Sicherheitsmanagement und Unternehmenssicherheit" an der Deutschen Universität für Weiterbildung Berlin soll die Absolventen in die Lage versetzen, ganzheitliche Sicherheitskonzepte zu entwickeln und sie in Unternehmen, Einrichtungen und Behörden zu implementieren. Begründet in einem interdisziplinären Ansatz, soll er eine systematische Perspektive auf Fragen der Sicherheit von Personen und Sachwerte richten. Geplante Vertiefungsrichtungen fokussieren auf Sicherheitsmanagement und Unternehmenssicherheit.

2.3 MÖGLICHE MODELLE FÜR DIE VERZAHNUNG VON AUS- UND WEITERBILDUNG




Aus der Vielzahl der aktuell praktizierten oder in Erprobung befindlichen Methoden zur Verzahnung von Aus- und Weiterbildung betrachtet der Autor folgende vier als wesentlich:

2.3.1 MODULARISIERUNG

Das Prinzip der Modularisierung wird bildungspolitisch kontrovers diskutiert:

- als Teilqualifikation innerhalb von Ausbildungsberufen,
- als Wechselmöglichkeit zwischen gleichwertigen Formen der Berufsausbildung,
- als pädagogische Methodik für eine praxisorientierte Ausbildung.

Gerade Letzteres beherrscht zunehmend die Ausbildungspläne, bietet aber das Risiko neuer Unflexibilität bei starrer Abarbeitung. Das von der ATB Chemnitz in mehreren Modellversuchen erprobte Konzept des Lernpfades verbindet die Vorteile der Modularisierung mit denen der Bedarfsgerechtheit (aus Arbeitssituation oder Arbeitsanforderung abgeleitet).

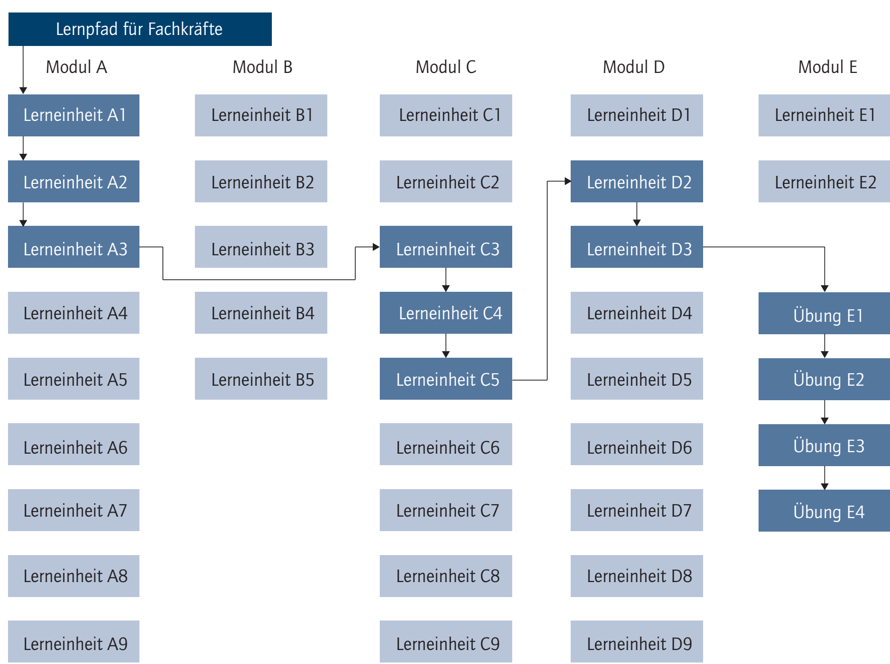
Lernpfade sind individuelle Lernwege, die sich aus vorhandenen sowie vom konkreten Bedarf abgeleiteten und anzueignenden Kompetenzen generieren. Die Qualifizierungsinhalte werden flexibel in Abhängigkeit der Bedarfe individuell zusammengestellt bzw. absolviert.





Abbildung 2 verdeutlicht schematisch an einem Beispiel Möglichkeiten zur Verbindung einzelner Lernhilfen und die Anordnung von einzelnen Konzepten zu einem Curriculum bei einer Abfolge von Lernschritten mit Lernsequenzen und vertiefenden Informationen.

Abbildung 2: Beispiel Lernpfadkonzept im Rahmen einer Projektarbeit






2.3.2 ZUSATZQUALIFIKATIONEN

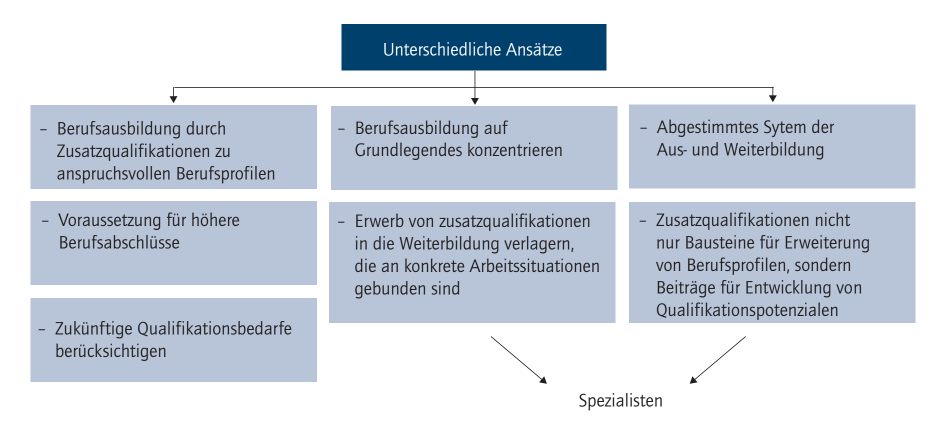
Zusatzqualifikationen bilden ein wichtiges Moment der Verzahnung von Aus- und Weiterbildung. Sie gestatten eine praxisnahe Differenzierung im Sinne einer individuellen Profilbildung, zum Beispiel eine integrative Aufgabenwahrnehmung von Produktion und Sicherheit. Somit entstehen Voraussetzungen für einen klassischen hierarchischen Aufstieg ebenso wie neue Mobilitätspfade und Karrieremuster. Neue prozessorientierte Formen der Arbeitsorganisation (zum Beispiel Gruppenarbeit) werden durch den Erwerb zusätzlicher sozialer Qualifikationen erst ermöglicht. Dazu existieren unterschiedliche Ansätze; drei gilt es zu beleuchten (Abbildung 3).







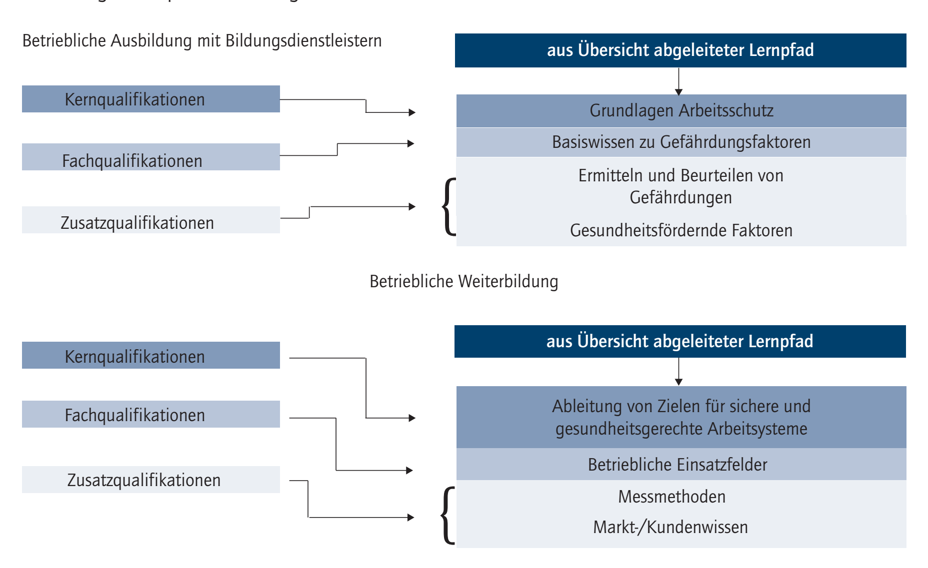
Abbildung 3: Ansätze für Zusatzqualifikationen



Zwei der gezeigten Ansätze stellen Lösungsmöglichkeiten für den von der Industrie zunehmend beklagten Fachkräftemangel dar, der sich zumeist als ein Mangel an Fachkräften mit Spezialwissen (Spezialisten) erweist. Abbildung 4 zeigt ein Beispiel der Verzahnung von Aus- und Weiterbildung mittels Zusatzqualifikation.




Abbildung 4: Beispiel Verzahnung im Bereich Arbeitsschutz







2.3.3 FLEXIBILITÄT

Die Entwicklung und Umsetzung von Lernkonzepten der Aus- und Weiterbildung für Unternehmen mit innovativen Fertigungstechnologien benötigt ein ausreichendes Maß an Flexibilität.

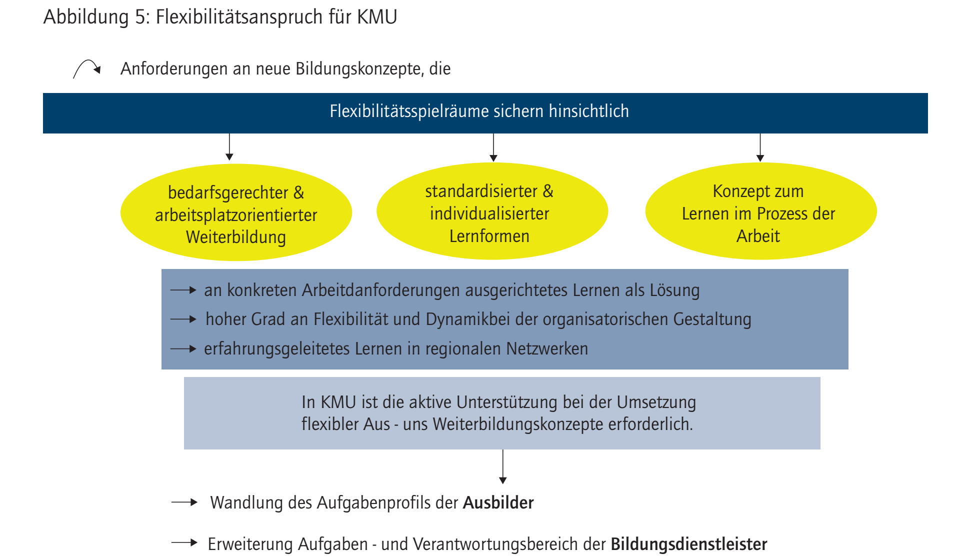
Der Auf- und Ausbau von Handlungskonzepten für die Verzahnung von Aus- und Weiterbildung tangiert zwei Flexibilitätsbereiche:

- betriebliche Gestaltungsanforderungen, die folgende Spezifika berücksichtigen: berufsspezifisch, praxisorientiert, betriebsspezifisch, arbeitsplatzbezogen, persönlichkeitsbezogen, leistungsbezogen;
- Gestaltung der Berufsbilder in einer Einheit von Kern-, Fach- und Zusatzqualifikation sowie von Einsatzgebieten.

Das Fachpersonal für sicherheitsrelevante Technologien bildet einen wesentlichen Erfolgsfaktor zur Erhaltung und Steigerung der Wettbewerbsfähigkeit von kleinen und mittleren Unternehmen (KMU). Den daraus abgeleiteten Flexibilitätsanspruch enthält.




Abbildung 5: Flexibilitätsanspruch für KMU



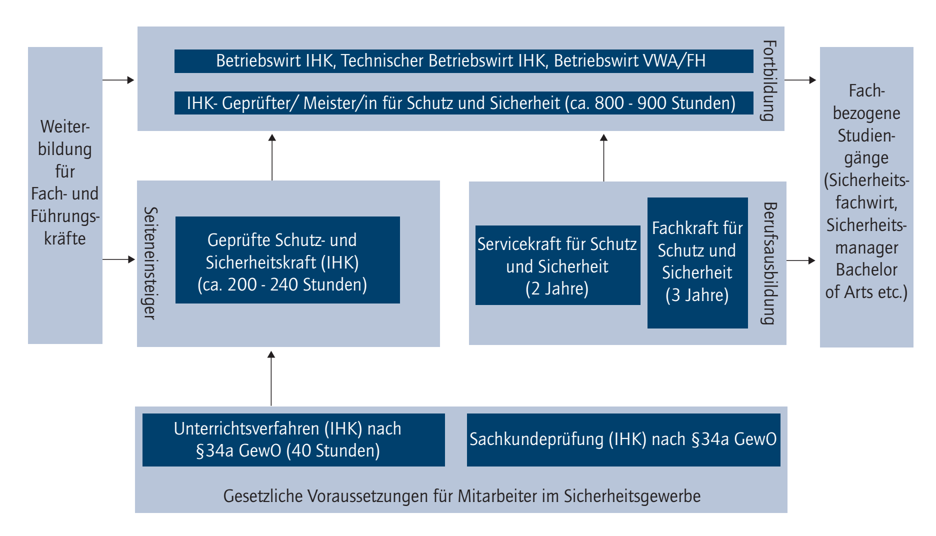




2.3.4 GESTALTUNGSOFFENHEIT

Die hohe Qualität, die von Fachkräften auf dem Sicherheitssektor (von der Sicherheitsbranche bis zu Beauftragten für einzelne Sicherheitsgebiete) absolut erfolgsentscheidend ist, steht und fällt mit der Souveränität und Kompetenz der Mitarbeiter/innen. Ein gestaltungsoffenes und gestuft durchgängiges Aus-, Fort- und Weiterbildungssystem trägt dazu bei, die gewünscht hohe Qualität in der Sicherheit zu erreichen (Abbildung 6).

Abbildung 6: Aus-, Fort- und Weiterbildungssystem auf dem Gebiet der Sicherheit






2.4 ZUSAMMENFASSUNG UND SCHLUSSFOLGERUNGEN

Sicherheit und Kompetenzerwerb sind untrennbar verbunden – fachliche Qualifizierung allein reicht nicht aus; erst durch die Entwicklung von Kompetenzen bei Individuen und Organisationen gibt es gute und nachhaltige Produkt- und Prozessqualität.

Viele Arbeitsplätze in der Sicherheitswirtschaft zeichnen sich aus durch:

- stärker kompetenzgeprägte und weniger qualifikationsbezogene Arbeitsweisen, wohl wissend, dass zum Aufbau von Kompetenzen Qualifikationsabschlüsse eine unmittelbare Voraussetzung sind;
- die Notwendigkeit zum berufsbegleitenden Neu- und Weiterlernen.



Das traditionelle Verständnis von einer Erstausbildung und dem nachfolgenden Erwerb von passgenauen Zusatzqualifikationen ist besonders im Sicherheitsbereich durch viele Facetten zu erweitern, wie die Kurzanalyse und die beispielhafte Modellentwicklung belegen.

Dazu existieren vielfältige Forschungsfragen und -Themen:

- Wie viel „Sicherheit" muss/kann/soll mit der Bildung in welchen Bereichen vermittelt werden (Informationen/Forschungsergebnisse → Lerninhalte → Lernprozess → Kompetenzaufbau → praktische Anwendung)?
- Wie kann das Interesse am Thema bzw. in der Bildung erhöht werden?
- Neben sachbezogener Forschung ist auch an Bildungsforschung (Kompetenzentwicklung) zu denken.
- Was sind die Schlüsselkompetenzen für Sicherheit (Safety/Security)? Wie können diese vermittelt werden?
- Wie ist die erforderliche Verzahnung von Aus- und Weiterbildung auf den Sicherheitsgebieten und deren Anwendungsfeldern zukunftsfähig zu gestalten? Reicht Modularisierung für neue Lernprozesse aus?





Der Anlass für die erforderliche ständige Kompetenzerweiterung der Mitarbeiter mit Sicherheitsaufgaben ist die Notwendigkeit, sich rasch auf neue Herausforderungen einzustellen und die Bedürfnisse des Marktes, der Kunden und der Gesellschaft zu befriedigen.

2.5 LITERATURVERZEICHNIS

Bundesgesetzblatt 2008
Bundesgesetzblatt 2008 Teil I, Nr. 21, ausgegeben zu Bonn, 31.05.2008. Köln: Bundesanzeiger Verlag, S. 93 ff.

BIBB 2008
Datenblätter der Datenbank Aus- und Weiterbildungsstatistik des Bundesinstituts für Berufsbildung (BIBB) auf Basis der Berufsbildungsstatistik des Statistischen Bundesamtes (StBA), Erhebung zum 31. Dezember.

LuftSiSchulV 2008
Luftsicherheits-Schulungsverordnung (LuftSiSchulV), 02.04.2008. URL: http://www.transportrecht.de/transportrecht_content/1209473147.pdf [Stand: 22.7.2009].





Österreichische Akademie der Wissenschaften 2005
Österreichische Akademie der Wissenschaften: Sicherheitsforschung – Begriffsfassung und Vorgangsweise für Österreich, Wien, 2005.

Risch 2008
Risch, W.: Bedingungen und Voraussetzungen in KMU für die Nutzung der Effekte aus der Verzahnung von Aus- und Weiterbildung, (itf-Symposium, Schwerin 22.11.2008), Schwerin, 2008 – Tagungsband.

Risch/Raßbach 2008
Risch, W.; Raßbach, K.: Kurzrecherche. Das Thema Sicherheit in der Aus- und Weiterbildung von Fachkräften, (Manuskript), Chemnitz, 2008.

Thoma 2008
Thoma, K.: Sicherheitsforschung in einer globalen, vernetzten Welt, (Parlamentarischer Abend der FhG, Berlin 20.02.2008), Berlin 2008 – Tagungsband.

Wermann et al. 2009
Wermann, L. et al.: Lead facility Services Globally (Luftsicherheitstage Berlin, 11.-12.02.2009) Berlin, 2009 – Tagungsband.








3 KERNKOMPETENZEN FÜR DIE SICHERHEIT: WISSENSCHAFTLICH-TECHNISCHE KOMPETENZ BRAUCHT LEHRE UND FORSCHUNG – EIN BEISPIEL

NORBERT PFEIL

3.1 DIE DECHEMA-INITIATIVE „KOMPETENZSICHERUNG UND -WEITERENTWICKLUNG IN DER SICHERHEITSTECHNIK"

Mit seinem Positionspapier „Kompetenzsicherung und -weiterentwicklung in der Sicherheitstechnik" startete der inzwischen in die ProcessNet-Fachgemeinschaft Sicherheitstechnik aufgegangene DECHEMA/GVC-Forschungsausschuss „Sicherheitstechnik in Chemieanlagen" im März 2004 eine Initiative zum Kompetenzerhalt, die trotz grundsätzlicher Anerkennung und zahlreicher Folgeaktivitäten noch nicht den gewünschten Erfolg gezeigt hat. Die grundsätzliche Zustimmung zu einer solchen Initiative bezieht sich inzwischen nicht nur auf die Sicherheitstechnik in Chemieanlagen, sondern auch auf weitere klassische Studienfächer, in denen in gleicher Weise ein Kompetenzverlust befürchtet oder schon beobachtet wird. Erfolgreich hat sich hingegen Anfang 2007 ein Kompetenzverbund Strahlenforschung etabliert.

Der vorliegende Beitrag informiert im Detail über die Initiative „Kompetenzsicherung und -weiterentwicklung in der Sicherheitstechnik", ergänzt damit frühere Publikationen zu diesem Thema[1] und soll anregen, die Beweggründe für diese Initiative sowie ihre Lösungsansätze auf die politische Ebene zu tragen. Nachfolgend ist das Positionspapier im vollständigen Wortlaut aufgeführt.

[1] Pfeil 2007 und Muschelknautz/Pfeil/Schönbucher 2009.





KOMPETENZSICHERUNG UND -WEITERENTWICKLUNG IN DER SICHERHEITSTECHNIK

Positionspapier
des DECHEMA/GVC-Forschungsausschusses „Sicherheitstechnik in Chemieanlagen"
März 2004

Die Chemische Industrie und der Apparatebau in der Bundesrepublik repräsentieren einen bedeutenden Teil der Wirtschaftskraft und der Beschäftigung von Arbeitskräften in Deutschland. Notwendige Voraussetzung für die Weiterentwicklung dieses Wirtschaftszweiges ist, dass die in Deutschland geplanten, gebauten und betriebenen Produktionsanlagen weiterhin sicherheitstechnisch auf hohem Niveau sind. Sichere Anlagen bewahren nicht nur Mensch und Umwelt vor Schäden, sie arbeiten auch wirtschaftlich, da jeder Schaden Produktionsausfall und Vernichtung von Werten bedeutet. In diesem Sinne fördert die Sicherheitstechnik ein ganzheitliches Prozessverständnis.



Die Akzeptanz dieser Industriezweige ist in besonders sensibler Weise davon abhängig, inwieweit Unfälle mit weitreichenden Auswirkungen durch Brände, Explosionen oder Freisetzungen von Gefahrstoffen in die Luft oder in Gewässer auftreten bzw. auftreten können. Daher ist es notwendig, dass Planung und Betrieb dieser Anlagen sicherheitstechnisch auf höchstmöglichem Niveau erfolgen. Die Auswertung von Ereignissen und insbesondere Störfällen belegt – auch im europäischen und internationalen Vergleich – das bereits erreichte hohe Sicherheitsniveau in der Bundesrepublik Deutschland. Dies kann umso mehr als Wettbewerbsvorteil genutzt werden, je höher die Sicherheit und der Umweltschutz in der Öffentlichkeit bewertet werden und der geleistete Aufwand im Wettbewerb der Industrieprodukte angemessen honoriert wird. Dieses gilt es zu erhalten und möglichst auszubauen.



Selbstverständlich sind Prozess- und Anlagentechnik – wie jede andere Technik auch – einer dynamischen Entwicklung unterworfen. Dem muss auch die Sicherheitstechnik Rechnung tragen. Die Sicherheitstechnik muss ein integraler Bestandteil der chemischen und verfahrenstechnischen Hochschulausbildung sein, deren hohes Niveau auf Dauer nur in der Einheit von Forschung und Lehre gewährleistet werden kann. (Siehe „Lehrprofil Sicherheitstechnik", herausgegeben vom DECHEMA/GVC-Fachausschuss „Sicherheitstechnik in Chemieanlagen"). Bekanntermaßen kann ein Lehrangebot auf dem benötigten hohen Niveau nur mittels einer fundierten Forschung aufrechterhalten werden, damit der Wirtschaft ausreichend qualifizierte Hochschulabsolventen zur Verfügung gestellt werden können. Auch ist die sicherheitstechnische Grundlagenforschung im Unterschied zur ausschließlich von der Industrie getragenen Forschung der allgemeinen Nutzung zugänglich.





Der DECHEMA/GVC-Forschungsausschuss „Sicherheitstechnik in Chemieanlagen" beobachtet mit Sorge, dass abweichend von den dargestellten Erfordernissen die Sicherheitstechnik nicht mehr in dem Maße weiterentwickelt wird, wie es wegen ihrer Bedeutung an sich und insbesondere auch im Hinblick auf die strategischen volkswirtschaftlichen Vorteile für angemessen gehalten wird. Die Ursachen werden u. a. gesehen in

- der fehlenden Forschungsförderung für Themen der Sicherheitstechnik durch die öffentliche Hand,
- der Entwicklung, dass in der Vergangenheit primär sicherheitstechnisch orientierte Lehrstühle und Institute heute zunehmend auf andere Forschungsbereiche ausgerichtet werden,
- den mit dem Rückgang universitärer Forschungskapazitäten auf dem Gebiet der Sicherheitstechnik einhergehenden Einschränkungen bei den Ausbildungsinhalten und -möglichkeiten und
- dem somit häufig unzureichenden sicherheitstechnischen Basiswissen von Hochschulabgängern, das zusätzlich durch externe Fachseminare oder firmenintern vermittelt werden muss oder andernfalls fehlt,
- einer deutlich gesunkenen Zahl der Studierenden in der Verfahrenstechnik und in der Technischen Chemie und damit auch in der Sicherheitstechnik,
- dem zunehmend begrenzteren Handlungsspielraum der deutschen Industrie für Forschung und Entwicklung auch in der Sicherheitstechnik, u. a. als eine Folge des globalen Wettbewerbs, der zum Teil durch nicht einheitliche internationale Rahmenbedingungen verschärft wird.





Um einem Verlust an Kompetenz auf dem Gebiet der Sicherheitstechnik vorzubeugen, schlägt der DECHEMA/GVC-Forschungsausschuss „Sicherheitstechnik in Chemieanlagen" vor:

1. Die Nutzung des DECHEMA/GVC-Forschungsausschusses „Sicherheitstechnik in Chemieanlagen" in der Wahrnehmung der Aufgaben eines Kompetenzverbundes aus

   - Planern und Betreibern von Chemieanlagen,
   - Vertretern von Forschungsinstituten,
   - Vertretern aus Behörden des Bundes und der Länder.





Dieser Verbund soll

- Ausbildungsdefizite aufzeigen und auf ihre Beseitigung hinwirken,
- Schwerpunktthemen für die sicherheitstechnische Forschung formulieren und nach Priorität bewerten sowie
- dazu beitragen, vorhandenes Wissen, Erfahrungen und neue Erkenntnisse zur Sicherheitstechnik – insbesondere für KMU – verfügbar und deren Anwendung verständlich zu machen.

2. Eine Initiative zur Sicherstellung der Finanzierung notwendiger Forschungsvorhaben in der Sicherheitstechnik

   Hierzu müssen Vertreter von Ministerien, die über die Vergabe von Fördermitteln zu befinden haben, des VCI sowie Entscheidungsträger der Großchemie an einen Tisch gebracht werden.

Mit diesen Vorschlägen möchte der DECHEMA/GVC- Forschungsausschuss „Sicherheitstechnik in Chemieanlagen" einen Beitrag für die Kompetenzsicherung und -weiterentwicklung in der Sicherheitstechnik in Deutschland leisten. Im Rahmen der Zukunftssicherung sind die Politik und die Industrie aufgerufen, die vorgenannten Anregungen aufzugreifen.

Kernaussage des Positionspapiers ist also die Sorge, dass die sicherheitstechnische Forschung mangels Fördermöglichkeiten für die Hochschulen an Attraktivität verliert und darunter auch die Lehre leidet, mit der Folge, dass der Wirtschaft entsprechend qualifizierte Hochschulabsolventen nicht mehr zur Verfügung gestellt werden.

Vorbereitet durch eine erste Bitte um Stellungnahme zum Positionspapier hatte die DECHEMA zum 19. November 2004 Vertreter aus der Wirtschaft, aus der Wissenschaft, von Verbänden und Vereinigungen sowie von Bundes- und Landesministerien zu einem Rundtischgespräch zu diesem Thema eingeladen. Nicht teilgenommen hatte das BMBF unter Hinweis darauf, dass Sicherheitsaspekte im Rahmen von Verbundprojekten zu neuen Technologien berücksichtigt würden, die Behandlung spezieller sicherheitstechnischer Fragestellungen aber in der Hand der Industrie bleiben müsse.

In der einführenden Präsentation[2] wurde unter anderem deutlich gemacht, welche Auswirkungen die öffentliche Förderung sicherheitstechnischer Themen auf die Forschungslandschaft hat. Eine solche Förderung hatte es zwischen 1980 und 1995 gegeben. Bedarf wurde seinerzeit unter anderem wegen einer Reihe von Unfällen – außerhalb Deutschlands – gesehen. In dieser Zeit wurde die Sicherheitsforschung national durch steigende Fördersummen bis jährlich 14 Millionen DM unterstützt. Zeitgleich

2 Muschelknautz/Pfeil 2004.



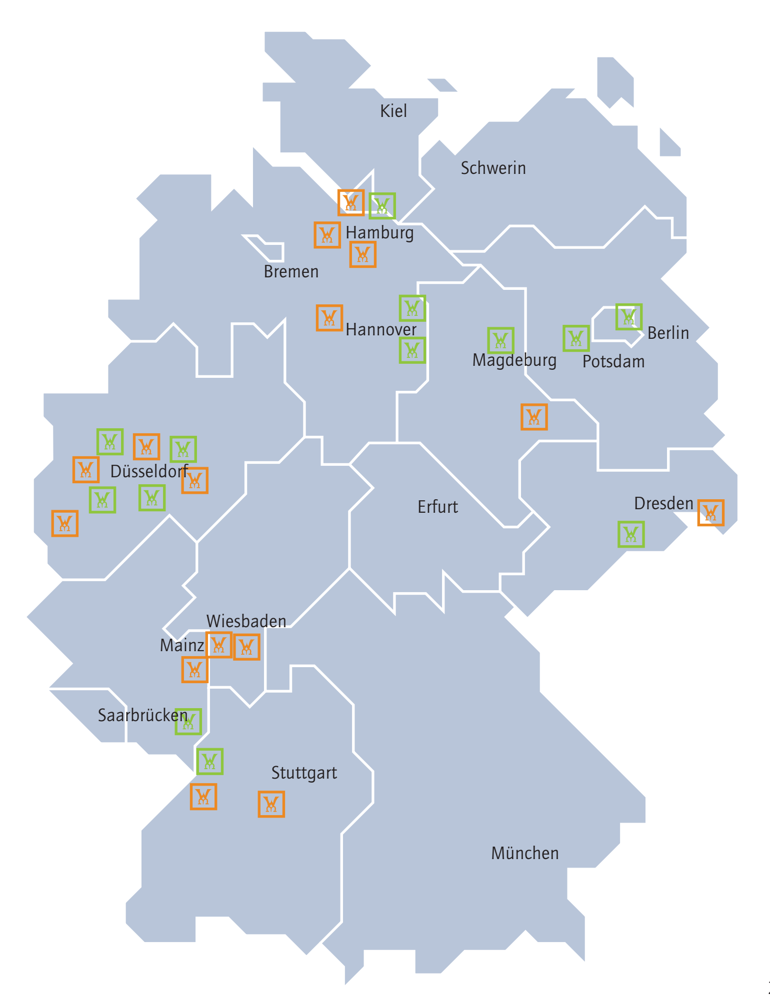


wurde dieses Gebiet durch ein europäisches Forschungsprogramm „Major Technological Hazards" mit 10 Millionen DM pro Jahr gefördert. Nach Einstellen dieser Förderprogramme ging das Interesse an sicherheitstechnischen Themen dieser Art zurück. Abbildung 1 zeigt eine Landkarte der seinerzeit aus der Forschungsförderung einschlägig bekannten Institute (grün und rot), von denen 2004 nur noch die grün markierten in der sicherheitstechnischen Forschung aktiv waren. Auch wenn die zugrunde liegende Erhebung keinen Anspruch auf Vollständigkeit erhebt, ist die Aussage eindeutig. In der Zwischenzeit hat die Zahl der mit der Sicherheit verfahrenstechnischer Anlagen befassten deutschen Forschungsinstitute weiter abgenommen. Sichtbare Konsequenzen sind beispielsweise eine abnehmende Zahl sicherheitstechnischer Beitragseinreichungen zu Tagungen und die unbefriedigende Bewerberlage bei einschlägigen Stellenausschreibungen.

Abbildung 1 Sicherheitstechnische Forschung in Deutschland – Institutslandschaft bis 1995 (rot und grün) und 2004 (grün)









Die Teilnehmer des Runden Tisches begrüßten die Initiative des Forschungsausschusses: Die Situation der Sicherheitstechnik in Deutschland wird sowohl mit dem gegenwärtigen Stand als auch in der zu erwartenden Entwicklung richtig eingeschätzt. Das Sicherheitsniveau in Deutschland ist hoch und es muss als Wettbewerbsvorteil verstanden und genutzt werden. Von deutschen Produkten und deutscher Technik wird erwartet, dass sie Qualität haben und sicher sind. Dieses Image darf nicht geschädigt werden. Gleiches gilt auch für die Akzeptanz der Technik und insbesondere der Chemie in der Öffentlichkeit. Ein wesentlicher Faktor für den Erhalt der gegenwärtig vorhandenen sicherheitstechnischen Kompetenz ist die Ausbildung. Die Wirtschaft und insbesondere die kleinen und mittleren Unternehmen (KMU) benötigen mit sicherheitstechnischem Grundwissen gut ausgebildete Ingenieure und Naturwissenschaftler. Eine solche Ausbildungssituation ist wegen der Verknüpfung von Forschung und Lehre nur zu erreichen, wenn die Befassung mit sicherheitstechnischen Fragen für die Hochschulen attraktiv ist.

Das Rundtischgespräch bestätigte die Bedeutung der expliziten Präsenz des Themas „Sicherheitstechnik“ in der öffentlichen Forschungsförderung für den Kompetenzerhalt, die beteiligte Wirtschaft zeigte mögliche Wege zu einer Kofinanzierung einer öffentlich geförderten Sicherheitstechnik auf und die Teilnehmer verständigten sich auf die Durchführung eines zweiten Rundtischgesprächs unter der Voraussetzung, dass die Teilnahme des BMBF erreicht werden kann.




Nach dem Rundtischgespräch wurde wiederholt der Kontakt zum BMBF gesucht. In Vorbereitung dieser Kontakte wurde die dem Runden Tisch vorgelegte ursprüngliche Sammlung sicherheitstechnischer Forschungsthemen des Forschungsausschusses aus Industriesicht priorisiert und zu vier Themenschwerpunkten zusammengefasst: Risiko und Zuverlässigkeit, Modellierung und Prozesssimulation, sicherheitstechnische Bewertung neuer Technologien, Kompetenzvermittlung. Das vollständige Papier findet sich im nachfolgenden Kasten.

Juli 2005

INITIATIVE KOMPETENZSICHERUNG UND -WEITERENTWICKLUNG IN DER SICHERHEITSTECHNIK – PRIORITÄRER FORSCHUNGSBEDARF AUS INDUSTRIESICHT

EINFÜHRUNG

Mit seinem Positionspapier „Kompetenzsicherung und -weiterentwicklung in der Sicherheitstechnik“ hat der DECHEMA/GVC-Forschungsausschuss „Sicherheitstechnik in Chemieanlagen“ dargelegt, dass der Erhalt des in Deutschland hohen Sicherheitsniveaus verfahrenstechnischer Anlagen einer gezielten Forschungsförderung insbesondere als Voraussetzung für eine zielgerichtete sicherheitstechnische Qualifizierung im Rahmen der einschlägigen Hochschulausbildungen bedarf.





Diese Position wurde bestätigt in einem Rundtischgespräch am 19. November 2004 bei der DECHEMA in Frankfurt am Main, in dem seitens der Wirtschaft Bereitschaft signalisiert wurde, hier gemeinsam mit dem Staat Lösungen zu suchen und finanzielle Beiträge zu leisten.

Aus diesem Grund wurde auf der Basis der von den Arbeitsausschüssen des DECHEMA/GVC-Forschungsausschuss „Sicherheitstechnik in Chemieanlagen" zusammengestellten und am 19.11.2004 beim Rundtischgespräch verteilten Liste sicherheitstechnischer Forschungsthemen in den beteiligten Industrieunternehmen eine Abfrage nach prioritären Forschungsthemen durchgeführt. In Auswertung dieser Abfrage ergeben sich vier Schwerpunkthemen, die nachfolgend beschrieben sind.

A RISIKO

Der Begriff Risiko hat eine zentrale Bedeutung in der chemischen Sicherheitstechnik. Während er früher überwiegend qualitativ verwendet wurde, geht heutzutage der Trend eindeutig hin zur Quantifizierung. Dies betrifft einerseits das so genannte „Land Use Planning", das z. B. in Großbritannien und den Niederlanden schon seit geraumer Zeit mit quantifizierenden Risikoermittlungen hinterlegt wird. Auch fordert die IEC 15611 bereits heute den quantitativen Nachweis der Verfügbarkeit von sicherheitstechnischen Abschaltketten.




Der Forschungsausschuss Sicherheitstechnik in Chemieanlagen sieht in der Quantifizierung der Zuverlässigkeit von sicherheitsrelevanten Ausrüstungen eine zentrale Zukunftsaufgabe. Die Analyse und die Optimierung der Zuverlässigkeit darf sich dabei nicht nur auf sicherheitstechnische Abschaltungen konzentrieren.

Es wurde die Vision entwickelt, dass alle Komponenten einer Chemieanlage, die ausfallgefährdet sind und bei Ausfall sicherheitsrelevante Eingriffe wie z. B. Abblasen von Sicherheitsventilen oder Aktivierung von Abschaltungen nach sich ziehen, systematisch auf ihre Verfügbarkeit untersucht werden.

Mit Hilfe zu entwickelnder Methoden soll das Potential zur Optimierung ihrer Verfügbarkeit aufgezeigt werden. Wenn es gelingt, die Verfügbarkeit soweit zu verbessern, dass die Anforderungen der IEC 61508/61511 erfüllt werden, können die Anforderungen an eine Absicherung reduziert werden. Im Grenzfall kann auf eine Absicherung vollständig verzichtet werden.

Der wesentliche Fortschritt wird darin gesehen, dass die Ausfallwahrscheinlichkeit von Chemieanlagen wesentlich reduziert wird. Die damit verbundene Erhöhung der Anlagensicherheit stellt gleichzeitig einen großen wirtschaftlichen Vorteil durch deutlich erhöhte Anlagenverfügbarkeit dar. Außerdem können auf diese Weise konventionelle Absicherungseinrichtungen eingespart werden.





B MODELLIERUNG UND PROZESSSIMULATION

Methodik/Werkzeuge

Die moderne Verfahrenstechnik ist mit einem Anforderungsprofil konfrontiert, bei dem einerseits neue Prozesse in möglichst kurzer Zeit in die Produktion überführt werden sollen und andererseits bekannte und weiterhin relevante Verfahren soweit optimiert sind, dass auf empirischem Wege kaum noch eine Leistungssteigerung zu erzielen ist. Um diesen Anforderungen gerecht zu werden, sind vertiefte Einsichten in die Physik dieser Vorgänge erforderlich, die zu stärker differenzierten Prozessbeschreibungen und damit zu neuen Design- und Optimierungsmöglichkeiten führen. Da solche Beschreibungsansätze meist nicht mehr in überschaubaren Gleichungen oder Diagrammen zusammengestellt werden können, etablieren sich zunehmend computergestützte mathematische Werkzeuge wie die Prozesssimulation und die numerische Strömungssimulation, die (besser) als Computational Fluid Dynamics (CFD) bekannt sind.



Heute ist die CFD in der Verfahrenstechnik ein etabliertes Werkzeug zur Auslegung und Optimierung zahlreicher Prozesse sowie am aussichtsreichen Beginn der Bearbeitung von sicherheitstechnischen Problemstellungen wie z.B. reaktiver, mehrphasiger Strömungen einschließlich technischer Verbrennungsvorgänge. So ist es insbesondere möglich, lokale Informationen über Konzentrationen, Temperaturen, Strömungsgeschwindigkeiten, Turbulenz, Stoff- und Wärmeübertragung sowie chemische Reaktionen zu erhalten, was vielfach durch experimentelle Untersuchungen allein nicht möglich ist. Weiterhin sind Parameterstudien zur Untersuchung des Einflusses von z. B. Geometrie- und Betriebsparametern numerisch viel kostengünstiger durchführbar als durch vergleichbare Experimente. Ebenso kann die Maßstabsübertragung mit Hilfe von CFD erfolgreich bearbeitet werden.

Mit zunehmendem Einsatz von CFD wird die Vorhersagegenauigkeit von Modellen wachsen sowie die Beschreibung immer komplexerer Systeme möglich (s. unten). Je stärker sich eine realistische Beurteilung der Möglichkeiten und Grenzen der CFD in der industriellen verfahrenstechnischen Anwendung durchsetzt, um so mehr wird ein gezielter und Erfolg bringender Einsatz der CFD zum Standard werden. Hierdurch werden andererseits Modell- und Verfahrensentwicklungen in der CFD gefördert, bzw. werden Verbesserungen von physikalischen Modellen eintreten, die wiederum der Verfahrenstechnik zugute kommen.

Die weitere Entwicklung und Anwendung von CFD in der industriellen Praxis steht in engem Zusammenhang mit den verfügbaren Rechnerleistungen und der Weiterentwicklung von Modellen insbesondere zur Beschreibung von Impuls-, Stoff- und Wärmetransportprozessen. Die zu erwartende kontinuierliche Steigerung der Rechnerleistung wird die Einbeziehung zunehmend komplexer Modelle erlauben. Deshalb werden zukünftig auch Grobstruktursimulationen [LES: Large Eddy Simulations] so-





wie Direkte Numerische Simulationen [DNS: Direct Numerical Simulations] in zunehmendem Maße eingesetzt werden, um grundlegende Transportprozesse (einschließlich z. B. der Wärmestrahlung von Schadenfeuern) und Phänomene zu analysieren und dadurch die Modellierung für praktische Berechnungen zu verbessern.

Datenkompetenz
Detaillierte *experimentelle* Untersuchungen bleiben unersetzlich, um die Zuverlässigkeit der Modelle und numerischen Berechnungen zu überprüfen und sind das wichtigste Mittel zur quantitativen *Validierung*. Ein wesentliches Kriterium für die Verwendbarkeit eines Simulationsansatzes ist der Vergleich der Berechnungsergebnisse mit experimentellen Untersuchungen. Zukünftig muss der *Validierung* anhand von (Labor)Experimenten daher größere Aufmerksamkeit gewidmet werden als bisher. Es herrscht ein *Mangel* an (belastbar) gemessenen Stoffdaten, insbesondere aus den folgenden Gründen: (a1) Die in der CFD verwendeten Modellgleichungen (Bilanzgleichungen) enthalten eine Vielzahl von Stoffeigenschaften in Form von Parametern, meist noch von Druck und Temperatur abhängig. Für alle diese Stoffeigenschaften wie z.B. Viskosität, Diffusionskoeffizient, Dichte, Wärmeleitfähigkeit, Reaktionsgeschwindigkeitskonstanten, spezifische Wärmekapazität für jede beteiligte Stoffkomponente, müssen möglichst realistische (belastbare) Zahlenwerte vorliegen, häufig auch bei   erhöhten Temperaturen und Drücken. (a2) Häufig werden für verfahrenstechnische Berechnungen auch semi-empirische Modelle verwendet, die zusätzlich sicherheitstechnische Kenngrößen wie z.B. Explosionsgrenzen, Zündtemperaturen, Selbstentzündungstemperaturen, Mindestzündenergien enthalten können, deren Zahlenwerte für viele Stoffe bzw. Stoffgemische *nicht* (oder nicht belastbar) vorliegen. Unerlässlich ist, dass derartige Stoffdaten nicht nur – oft in Standard-Apparaturen – sorgfältig mit hohem Qualitätsstandard gemessen werden müssen, sondern darüber hinaus in entsprechenden Datenbanken gesichert gespeichert und jederzeit abrufbar sein sollten.

C SICHERHEITSTECHNISCHE BEWERTUNG NEUER TECHNOLOGIEN

In der Verfahrenstechnik gewinnen neue Technologien wie Mikroverfahrenstechnik, Membranverfahrenstechnik oder Nanoverfahrenstechnik zunehmend an Bedeutung. Dabei ist die sicherheitstechnische Bewertung und die Entwicklung geeigneter Absicherungen für neue Verfahren von zentraler Bedeutung.

So werden beispielsweise in der Mikroreaktionstechnik neuartige Plattentauscherreaktoren entwickelt, in deren Kanälen eine chemische Reaktion unter Anwesenheit eines Katalysators abläuft. Die Oxidation von Ethylen zu Ethylenoxid ist eine Beispielreaktion, die in den Mikrokanälen solcher Reaktoren mit außergewöhnlich hohen Konzentrationen effizient durchgeführt werden kann. Damit dies sicher geschieht, muss die sichere Grenzkonzentration genau bekannt sein. Weiterhin müssen





An- und Abfahrvorgänge sowie Störungsszenarien hinsichtlich Überschreitung dieser Grenzwerte sicherheitstechnisch bewertet werden. Die Hinzuziehung von sicherheitstechnischem Sachverstand bereits in einer frühen Phase bestimmt erfahrungsgemäß ganz wesentlich den weiteren Entwicklungsverlauf.

Gleiches gilt für neuartige Membranverfahren wie z. B. ionenleitende Hochtemperaturmembranreaktoren zur Erzeugung von Synthesegas aus Erdgas. Bei mechanischem Versagen der Membran kann es durch unkontrollierten Lufteintrag auf die heiße Reaktionsseite zu einem vollständigen Abbrand der Einheit führen. Die Entwicklung eines geeigneten Absicherungskonzepts bestimmt hier ganz wesentlich die ökonomische Attraktivität dieser Technologie gegenüber Standardverfahren.

Die Nanotechnologie ist ebenfalls eine Zukunftstechnologie, bei der insbesondere bei der Herstellung und der Anwendung der nanoskaligen Partikel sicherheitstechnische Aspekte kompetent und in einem frühen Stadium betrachtet werden müssen.

D KOMPETENZVERMITTLUNG

Neben der Qualifizierung der Hochschulausbildung und der dafür notwendigen Kompetenz in Einheit von Forschung und Lehre sieht das Positionspapier des DECHEMA/GVC-Gemeinschaftsausschusses Handlungsbedarf hinsichtlich des Erhalts und der Vermittlung von vorhandenem Wissen, Erfahrungen und neuen Erkenntnisses. Es genügt nicht, dass die notwendige Kompetenz zur Beantwortung sicherheitstechnischer Fragestellungen in der Summe vorhanden ist, sie muss im erforderlichen Umfang auch dort verfügbar sein, wo sie benötigt wird. In diesem Sinne wird auch die Förderung von der Kompetenzvermittlung als prioritär angesehen.




Im Rahmen mehrerer Treffen mit dem BMBF waren sich die Gesprächspartner einig, dass der Kompetenzerhalt in der Sicherheitstechnik gewährleistet sein muss. Das BMBF sah zunächst realistische Möglichkeiten, das Anliegen der DECHEMA-Initiative in ein nationales, das 7. EU-Forschungsrahmenprogramm flankierende Sicherheitsforschungsprogramm einzubringen, wofür es erforderlich wäre, dieses Anliegen mit der Förderungspolitik des BMBF in Deckung zu bringen. So könnten Themen aus dem Bereich „Safety“ – also technischer Sicherheit – nur berücksichtigt werden, wenn diese auch der „Security“ dienten – im Wesentlichen also der Abwehr von Bedrohungen durch Terrorismus oder extremistische Angriffe. Es wurde daher versucht, im Rahmen der 2006 vom BMBF durch-





geführten Workshops zur Entwicklung des nationalen Sicherheitsforschungsprogramms die vom Forschungsausschuss formulierten Themenschwerpunkte zu verankern, und zwar unter dem Stichwort Absicherung von Chemieanlagen als kritische Infrastrukturen im Sinne des BMI-Basisschutzkonzepts vom August 2005[3] mit den konkreten Themen:

- inhärent sichere Prozesse und Anlagen, Bewertung neuer Technologien und
- Untersuchung und Modellierung von Auswirkungsszenarien und Gegenmaßnahmen zur Berücksichtigung von Eingriffen Unbefugter in systematischen Gefährdungsanalysen einschließlich probabilistischer Vorgehensweisen.



Dieser Versuch ist nicht nur gescheitert, sondern es wurde parallel dazu vom BMBF im Frühjahr 2006 zum Anliegen der DECHEMA-Initiative klargestellt, dass es die gewünschte unmittelbare Förderung der Sicherheitstechnik nicht geben wird, da die Gewährleistung der erforderlichen Anlagensicherheit Aufgabe der Wirtschaft und die Förderung der Hochschullehre Aufgabe der Bundesländer sei. Das letzte Gespräch mit dem BMBF fand dann öffentlich statt, am 19. Mai 2006 als ACHEMA-Expertengespräch. Die Positionen der Vertreter der DECHEMA-Initiative und des BMBF wurden noch einmal ausgetauscht und begründet; eine Annäherung konnte nicht erreicht werden. Damit war klar, dass weitere Aktivitäten nur noch dann Erfolg zeigen können, wenn die politische Ebene für die DECHEMA-Initiative gewonnen wird. Ein Schreiben des Vorsitzenden des Forschungsausschusses im Oktober 2007 an die Bundesforschungsministerin konnte die erforderliche Sensibilisierung jedoch noch nicht erwirken.

Die Kommission für Anlagensicherheit, Beratungsgremium des Bundesministeriums für Umwelt, Naturschutz und Reaktorsicherheit, hat aus dem Explosionsunglück 2005 in einer Raffinerie in Texas City, USA Lehren für eine Weiterentwicklung der Sicherheitskultur gezogen und sich auch mit dem Thema „Fachkenntnisse und Ausbildungsstand" befasst. Dort heißt es: „Die KAS ist der Auffassung, dass durch die breite Einführung von Bachelor- und Masterstudiengängen und den damit verbundenen verkürzten Studienzeiten eine Reduzierung des Lehrstoffs zu Lasten der „Ergänzungsfächer" wie z. B. Anlagensicherheit nicht verbunden sein darf. Bei Nichtbeachtung ist mittel- bis langfristig mit einer Schwächung des Standes der Sicherheitstechnik zu rechnen [...]."[4] Damit stützt der KAS-Bericht die DECHEMA-Initiative aus anderer Sicht.

3 BMI 2005.
4 KAS 2008.





3.2 WAS IST DAS PROBLEM?

Ohne Zweifel ist es richtig, die öffentliche Forschungsförderung als politisches und wirtschaftliches Steuerungsinstrument einzusetzen. Im Schwerpunkt dieser Förderung liegen deshalb technische Innovationen, die neue oder verbesserte Produkte oder Verfahren erwarten lassen, die unsere Lebensqualität erhöhen und unsere Wirtschaft beflügeln sollen. Hierfür stehen Begriffe wie „Bio"-, „Nano"-, „Informations"- und „Kommunikationstechnologien", aber auch „Umwelt" und „natürliche Ressourcen".

Damit die eingesetzten Mittel die größtmögliche Wirkung entfalten, setzt die Forschungspolitik – auch national – seit einiger Zeit verstärkt auf große Verbundprojekte mit vielen Partnern. „Leuchtturmprojekte" sollen Exzellenz bündeln, Sichtbarkeit gewährleisten und zu innovationsfreundlichen Rahmenbedingungen beitragen. Auch das ist sicherlich richtig.

Nun müssen Hochschullehrer sich um Drittmittel bemühen. Drittmittel sind eines der üblichen Kriterien für den Nachweis der Qualität der Forschung an den Universitäten – und nicht nur dort – wie auch der einzelnen Hochschullehrer. Daher wenden sich diese vermehrt den Themen zu, die gefördert werden. Das ist ja auch die Absicht des forschungspolitischen Steuerungsinstruments. Nun ist für junge Menschen das Thema der Sicherheit von technischen Produkten, Prozessen, Anlagen und Systemen im Allgemeinen weniger attraktiv als die eingangs angesprochenen Zukunftstechnologien und -themen. Erst recht gilt dies, wenn in diesem Bereich tätige Hochschullehrer kein Geld zum Beispiel für potenzielle Doktoranden haben. So entsteht ein Nachwuchsproblem, in der Sicherheitstechnik wie in anderen industriellen Bereichen.



Es kann und soll hier nicht behauptet werden, es gäbe keine öffentliche Forschungsförderung für die technische Sicherheit. Rechtzeitig zur Vorbereitung des 7. Forschungsrahmenprogramms der Europäischen Union hat sich die European Technology Platform Industrial Safety (ETPIS) formiert und Anfang 2006 der Europäischen Kommission ihre „Strategic Research Agenda" vorgelegt. Diese zielt primär auf einen die verschiedenen Industriezweige übergreifenden Ansatz zur Gewährleistung industrieller Sicherheit. Die Ende 2006 gegründete Nationale Spiegelplattform Industrielle Sicherheit (DE-TPIS)[5] nimmt auf diesem Wege thematisch Einfluss auf die Entwicklung der europäischen Forschungsförderung. Auch dort wurden die DECHEMA-Initiative und der identifizierte Forschungsbedarf eingebracht. Es wird allerdings bezweifelt, dass derartige Förderstrukturen und -programme einen deutlich positiven Einfluss auf die sicherheitstechnische Forschung und damit auch auf die Lehre an Universitäten nehmen. Der Aufwand, sich erfolgreich über die entsprechenden Netzwerke in solche Programme einzubringen, ist

5 http://www.industrialsafety-tp.org/de/(S(2glbnomkaiu44aft3f0pqcuk))/default.aspx.





sehr hoch und für Hochschullehrer üblicherweise nicht attraktiv. Eine Signalwirkung für die sicherheitstechnische Forschung insbesondere an den Universitäten wird auf diese Weise nicht erreicht. Hier ist die Politik gefordert.

Ein positives Beispiel politischen Wirkens ist der Kompetenzverbund Kerntechnik.[6] Eingerichtet auf Empfehlung einer vom Bundesministerium für Wirtschaft und Technologie (BMWi) einberufenen Arbeitsgruppe zur nuklearen Sicherheits- und Endlagerforschung in Deutschland,[7] stimmen die beteiligten deutschen Forschungseinrichtungen ihre Forschungsarbeiten untereinander ab. In einer der Empfehlungen der Arbeitsgruppe heißt es, „dass die Forschungsarbeiten zur Reaktorsicherheit und zur Endlagerung an den Universitäten nicht zuletzt unter dem Gesichtspunkt des Erhalts wissenschaftlicher Kompetenz (Nachwuchsförderung) nachhaltig gefördert werden." Für die Kerntechnik gibt es also eine Forschungsförderung, die explizit zum Kompetenzerhalt und -ausbau und zur Förderung des wissenschaftlichen Nachwuchses ausgewiesen ist.

Die in dem Positionspapier des Forschungsausschusses „Sicherheitstechnik in Chemieanlagen" geschilderte Situation soll nicht mit der Situation in der Kerntechnik gleichgesetzt werden. Es sollte aber gelingen, aus der Einrichtung des Kompetenzverbundes Kerntechnik allgemeine Lehren zu ziehen. Sicher ist es richtig, die Forschungsförderung in starkem Maße als Steuerungsinstrument einzusetzen, das die Innovationskraft Deutschlands und Europas erhöht (Stichworte: 3-Prozent-Ziel des Lissabon-Gipfels und Hightech-Strategie der Bundesregierung). Es muss aber auch daran gedacht werden, dass Kompetenzen in grundlegenden Technikfeldern – nicht nur in den in diesem Beitrag betrachteten – erhaltenswert sind. Es ist offensichtlich, dass sich ein stabiles Kompetenzniveau in grundlegenden Feldern nicht von selbst einstellt. Dafür ist sicherlich nicht nur die aktuelle Forschungspolitik ursächlich, sondern auch die Attraktivität der „neuen" Themen insbesondere für junge Menschen, die gerade dabei sind, sich beruflich auszurichten.



3.3 WAS IST ZU TUN?

Die Politik sollte sich von den vorangehenden Gedanken überzeugen lassen, die Wirtschaft sollte ihren Beitrag zu ihrer Verwirklichung leisten. Seit Anfang 2008 gibt es acatech, die Deutsche Akademie der Technikwissenschaften. acatech will Politik, Wirtschaft und Gesellschaft mit kompetenten und unabhängigen Empfehlungen und Einschätzungen zur Seite stehen.[8] Der Forschungsausschuss „Sicherheitstechnik in Chemieanlagen" hatte die Initiative zum Kompetenzerhalt in der Sicherheitstechnik ergriffen. Die ProcessNet-Fachgemeinschaft Sicherheitstechnik tut ein Übriges und aktualisiert gegenwärtig

6 BMBF/BMU 2007.
7 BMWi-Evaluierungskommission 2000.
8 http://www.acatech.de/de/ueber-uns/profil.html.





das 1997 vom Forschungsausschuss herausgegebene Lehrprofil Sicherheitstechnik[9] nach den Vorgaben des Bologna-Prozesses. Das acatech-Themennetzwerk Sicherheit wird die vorgetragenen Gedanken aufgreifen und weitertragen. Vielleicht gelingt es auf diese Weise, deutlich zu machen, dass etwas getan werden muss, um der Marke „made in Germany", die immer noch für Qualität und Sicherheit steht, diese wichtigen Prädikate auf Dauer zu erhalten.

3.4 LITERATUR

BMBF/BMU 2007
Bundesministerium für Bildung und Forschung/ Bundesministerium des Innern: Gemeinsame Pressemitteilung BMBF und BMU: Bund stärkt Strahlenforschung. Nr. 037/07, Berlin, 07.02.2007. URL: http://www.bmu.de/pressemitteilungen/aktuelle_pressemitteilungen/pm/38654.php [Stand: 22.7.2009].

BMI 2005
Bundesministerium des Innern: Schutz Kritischer Infrastrukturen – Basisschutzkonzept, Berlin, 2005. URL: http://www.en.bmi.bund.de/Internet/Content/Common/Anlagen/Themen/Terrorismus/Basisschutzkonzept__fuer__Unternehmen,templateId=raw,property=publicationFile.pdf/Basisschutzkonzept_fuer_Unternehmen.pdf [Stand: 22.7.2009].



BMWi-Evaluierungskommission 2000
Bundesministerium für Wirtschaft und Technologie (BMWi), Evaluierungskommission: Nukleare Sicherheits- und Endlagerforschung in Deutschland, 21. Januar 2000. URL: http://www.fzk.de/fzk/groups/ptwte/documents/internetdokument/id_053681.pdf [Stand: 22.7.2009].

DECHEMA 1997
DECHEMA e.V.: Lehrprofil Sicherheitstechnik, Frankfurt am Main, 1997.

KAS 2008
Kommission für Anlagensicherheit beim Bundesministerium für Umwelt, Naturschutz und Reaktiorsicherheit: Empfehlungen der KAS für eine Weiterentwicklung der Sicherheitskultur - Lehren nach Texas Citiy, Bericht des Arbeitskreises Texas City, KAS-7. URL: http://www.sfk-taa.de/publikationen/kas/KAS_7.pdf [Stand: 22.7.2009].

[9] DECHEMA 1997.





Muschelknautz/Pfeil 2004
Muschelknautz, S.; Pfeil, N.: Kompetenzsicherung und -weiterentwicklung in der Sicherheitstechnik, (Präsentation 19. November 2004, Frankfurt am Main). URL: http://www.industrialsafety-tp.org/de/(S(2glbnomkaiu44aft3f0pqcuk))/downloads.aspx [Stand: 22.7.2009].

Muschelknautz/Pfeil/Schönbucher 2009
Muschelknautz, S./Pfeil, N./Schönbucher, A.: „Anlagensicherheit „made in Germany" – sichern wir unsere Kompetenz." In: Chemie Ingenieur Technik 81 (2009), Nr. 1-2, S. 37-40. URL: http://www3.interscience.wiley.com/cgi-bin/fulltext/121576444/PDFSTART [Stand: 22.7.2009].

Pfeil 2007
Pfeil, N.: Forschung für die Sicherheit, (P&A-Kompendium 2007/2008). URL: http://www.pua24.net/pi/index.php?StoryID=41&articleID=15917 [Stand: 22.7.2009].









4 EINSTELLUNGEN UND EINSCHÄTZUNGEN ZUKÜNFTIGER ENTSCHEIDER ZUM THEMA IT-SICHERHEIT: ERGEBNISSE UND SCHLUSSFOLGERUNGEN EINER DSIN-STUDIE 2008

GERHARD KNORZ

4.1 ZIEL DER STUDIE ZUR IT-SICHERHEIT

„IT-Sicherheit" ist nicht nur ein Schlagwort in Fach- und Tagespresse, sondern auch ein wesentlicher Aspekt für Erfolg, Misserfolg und Risiko von Anbietern und Nutzern von Informationstechnologie. Die Unsicherheit vieler Beteiligter im privaten und beruflichen Bereich ist groß und das Problembewusstsein und das Wissen um die richtigen Maßnahmen sind durchweg sehr heterogen entwickelt. Umso bedeutsamer ist die Frage, wie es in dieser Hinsicht um die IT-Entscheider von morgen steht – also um die Personen, die heute Informatik oder ein verwandtes Fach studieren. Wie wird dieser Personenkreis an den Hochschulen auf seine zukünftigen Verantwortlichkeiten vorbereitet?

Zu Beginn des neuen Jahrtausends fiel das Urteil der Gesellschaft für Informatik e.V. (GI) in dieser Hinsicht absolut negativ aus: „Als ‚in Inhalt und Umfang unangemessen' hat Jörg Maas, Geschäftsführer der Gesellschaft für Informatik e.V. (GI), die Ausbildung in der Informationssicherheit in Deutschland bezeichnet [... und er] forderte eine stärkere Berücksichtigung des Themas Sicherheit in der Informatikausbildung an Hochschulen", stellte die GI 2001 in einer Pressemeldung fest.[1] 2006 verabschiedete das GI-Präsidium eigene Empfehlungen zur Berücksichtigung der IT-Sicherheit in der schulischen und akademischen Ausbildung, die durchaus Einfluss auf den Ausbau der Informatik-Fachbereiche genommen haben.[2] Eine Untersuchung aber, die bei denen ansetzt, um deren Ausbildung es geht, also bei den Studierenden selbst, fehlte bislang. Wie sind sie für die Problematik der IT-Sicherheit sensibilisiert? Wie begegnet ihnen tatsächlich dieses Thema im Studium? Wie beurteilen sie das entsprechende Lehrangebot? Erkennen sie Handlungsbedarf und bei wem? Zu diesen Fragen gab es bestenfalls spekulative Antworten aus subjektivem Erfahrungskontext.

Aus diesem Grund haben der Branchenverband BITKOM und die Software AG als Handlungsversprechen für den Verein „Deutschland sicher im Netz" (DsiN) eine Studie bei der Hochschule Darmstadt in Auftrag gegeben.[3] Diese sollte im Rahmen einer explorativen Untersuchung eruieren, ob im Hinblick auf die IT-Entscheider von morgen alles „im grünen Bereich" liegt oder ob sich Befunde ergeben, die zu weiteren Aktivitäten

1 GI 2001, S. 1.
2 GI 2006.
3 Knorz 2008.





Veranlassung geben: zu weiter gehenden Untersuchungen, eventuell gar zu einem regelmäßigen Monitoring oder auch zu Handlungsempfehlungen an die Akteure in diesem Bereich.

4.2 GRUNDLAGE DER STUDIE

4.2.1 UMFRAGE

Die Studie beruht auf einem recht umfangreichen Online-Fragebogen mit 29 Fachfragen insbesondere zu den mit IT-Sicherheit verknüpften Bereichen Stellenwert, Ausbildung, Praxis und persönliches Umfeld, Computer- und Internet-Nutzung, Beruf und Karriere sowie Gesellschaft.

Der Fragebogen wurde während des Sommersemesters 2008 im Rahmen einer überschaubaren Web-Präsenz „IT-Sicherheit als Thema für zukünftige IT-Entscheider" unter der Adresse https://www.h-da.de/it-sicherheit online gestellt. Die Ansprache von Studierenden wurde mit Fachbereichen bzw. Lehrstühlen von jeweils drei Universitäten und drei Fachhochschulen verabredet.[4] Die Umfrage war darüber hinaus offen für jeden, der über die Web-Seiten der Hochschule Darmstadt oder der beteiligten anderen Hochschulen auf den Fragebogen bzw. die zugehörige Web-Seite gelangte und folgenden Text auf sich bezog:

„Interessieren Sie sich für Computer und Internet, und wollen Sie später in diesem Bereich beruflich tätig sein? Dann sind Sie hier richtig! Folgende Befragung zum Thema IT-Sicherheit richtet sich an Studierende, die Informatik studieren oder deren Studiengang teilweise auch Informatikwissen vermittelt."

Die Erfahrung zeigt, dass Online-Fragebögen mit ernsthaftem Erkenntnisinteresse und umfangreichen Frageninventar nicht das Problem haben, Trittbrettfahrer anzuziehen, sondern genügend Motivierte zu finden, die bereit sind, ihre Zeit zu investieren. Aus diesem Grund konnte die Umfrage ohne Bedenken offen ins Netz gestellt werden.

4.2.2 BEFRAGTE UND ANTWORTENDE

Die Untersuchung beruht auf insgesamt 359 Antworten. Gemessen am Bundesdurchschnitt sind Frauen mit einem Viertel der Antwortenden (26 Prozent) etwas überrepräsentiert. Erwartungsgemäß sind über 85 Prozent der Antwortenden zwischen 20 und 30 Jahren. Die Antworten kommen vornehmlich aus der Mitte Deutschlands (85 Prozent geben Hessen, Rheinland-Pfalz, Saarland oder Nordrhein-Westfalen als Bundesland an). Die Befragten besitzen alle einen eigenen Computer (100 Prozent), benutzen häufig das Internet (99,7 Prozent) und fast alle speichern auf ihrem Rechner auch vertrauliche Daten (85 Prozent).

4 Siehe Knorz 2008, S. 10.







Die Untersuchung spiegelt wider, dass der Bologna-Prozess mit der Einführung konsekutiver Studiengänge inzwischen weit fortgeschritten ist. Obwohl die meisten antwortenden Studierenden sich bereits in einem höheren Semester befinden, fällt die größte Anzahl der Antworten mit fast fünfzig Prozent auf Bachelorstudierende. Der Anteil von Studierenden in Diplomstudiengängen ist deutlich geringer (34 Prozent). Durchaus relevant mit zwölf Prozent sind Master-Studierende.

Die Antwortenden befinden sich überwiegend in einem fortgeschrittenen Studiensemester: über 40 Prozent studieren im vierten oder in einem höheren Studienjahr (also im achten oder in einem höheren Semester). Einigermaßen gleich verteilt ist das erste, zweite und dritte Studienjahr vertreten. Für aussagekräftige Ergebnisse der Studie erscheint die Verteilung auf die Studienphasen gut geeignet.

Ähnlich wie die Verteilung auf die Studienjahre stellt sich auch die Verteilung auf unterschiedliche Informatikanteile am Studium dar: Fast die Hälfte der Antwortenden ist der Kerninformatik mit mehr als 75 Prozent geschätztem Informatikanteil zuzuordnen. Die Studierenden mit geringeren Informatikanteilen verteilen sich etwa gleichmäßig. Diese Bandbreite schlägt sich insbesondere nieder in den Antworten zu Berufsorientierung, Tätigkeiten und Karrierezielen.





Die Studie zielt auf „zukünftige IT-Entscheider". Inwieweit stimmt die Vermutung, dass mit einem Studium tatsächlich eine Leitungsfunktion angestrebt wird? Insgesamt gilt, dass über drei Viertel aller Antwortenden eine Leitung auf Team-, Gruppen-, Abteilungs- oder Unternehmensebene anstreben (77 Prozent), nur 13 Prozent geben explizit an, keine Leitungsfunktionen zu wünschen.

4.3 EINSTELLUNGEN, SELBSTEINSCHÄTZUNG UND KOMPETENZEN DER STUDIERENDEN

Welche Haltung nehmen die zukünftigen IT-Entscheider ein? Für wie kompetent halten sie sich? Welche Bedeutung messen sie dem Thema zu? Wie verhalten sie sich? Diesen Fragen soll zuerst nachgegangen werden.

4.3.1 SELBSTEINSCHÄTZUNG VON KOMPETENZ UND PROBLEMBEWUSSTSEIN

Die Selbsteinschätzung zukünftiger IT-Entscheider ist durchaus positiv. Die weitaus überwiegende Mehrheit erklärt, analytisch zu wissen, was „IT-Sicherheit" bedeutet (63 Prozent). Fast alle anderen glauben zumindest zu wissen, was „IT-Sicherheit" ist, auch wenn sie sich eine Erklärung nicht zutrauen. Mit unter vier Prozent der Gesamtantworten fallen die beiden Kategorien „ich weiß nicht genau, was es bedeutet" und die Verschärfung „ich kenne IT-Sicherheit gar nicht" kaum ins Gewicht.





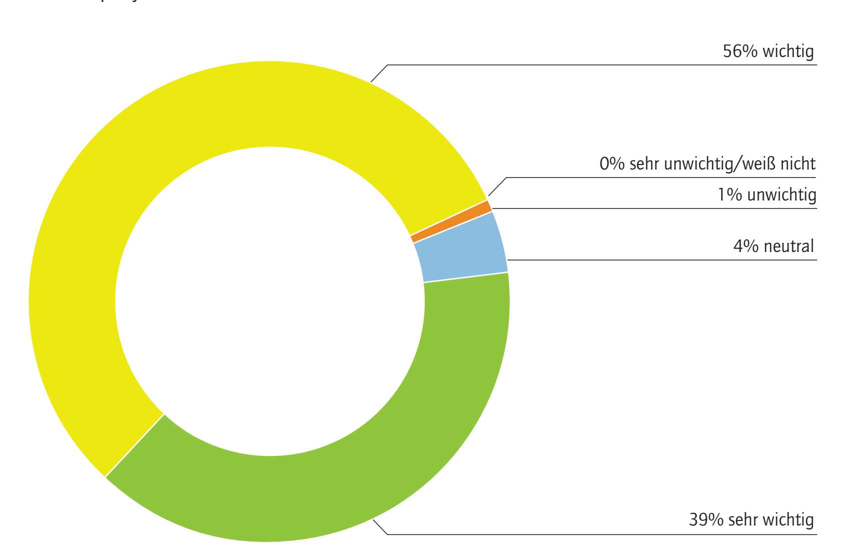
Dieses Ergebnis darf allerdings nicht unkritisch auf die Gesamtheit aller Studierenden von informatiknahen Studiengängen übertragen werden, da die Antworten von solchen Studierenden stammen, die sich der Mühe unterzogen haben, den der Studie zugrunde liegenden Fragebogen zu bearbeiten. Es handelt sich daher um eine Vorauswahl solcher Studierenden, die offenkundig ein gewisses Interesse am Thema „IT-Sicherheit" mitbringen. Diese Relativierung gilt auch für alle anderen Ergebnisse der Befragung.

Die zukünftigen IT-Entscheider testieren sich auch ein bemerkenswertes Ausmaß von Beschäftigung mit dem Thema: Fast drei Viertel der Antwortenden geben an, sich umfassend (23 Prozent) oder zumindest partiell (47 Prozent) mit dem Thema beschäftigt zu haben – und dies offensichtlich weitgehend unabhängig von ihrem Studium (siehe Abschnitt 4.4).

Wie wichtig ist den Studierenden die IT-Sicherheit? Abbildung 1 zeigt, dass im privaten Umfeld nahezu alle das Thema als sehr wichtig (39 Prozent) oder wichtig (57 Prozent) einordnen. Nur ca. fünf Prozent entscheiden sich für niedrigere Prioritäten. Im Detail zeigt sich, dass das Verhältnis der Nennungen „sehr wichtig" zu „wichtig" keineswegs mit wachsendem Informatikanteil steigt. Im Gegenteil: Studierende mit einem Informatikanteil unter 50 Prozent geben deutlich häufiger an, privat IT-Sicherheit „sehr wichtig" einzuschätzen, als dies Studierende mit größeren Informatikanteil bekunden.




Abbildung 1: Einschätzung der Bedeutung von IT-Sicherheit im privaten Umfeld. Farben der Darstellung nach Ampelsystem





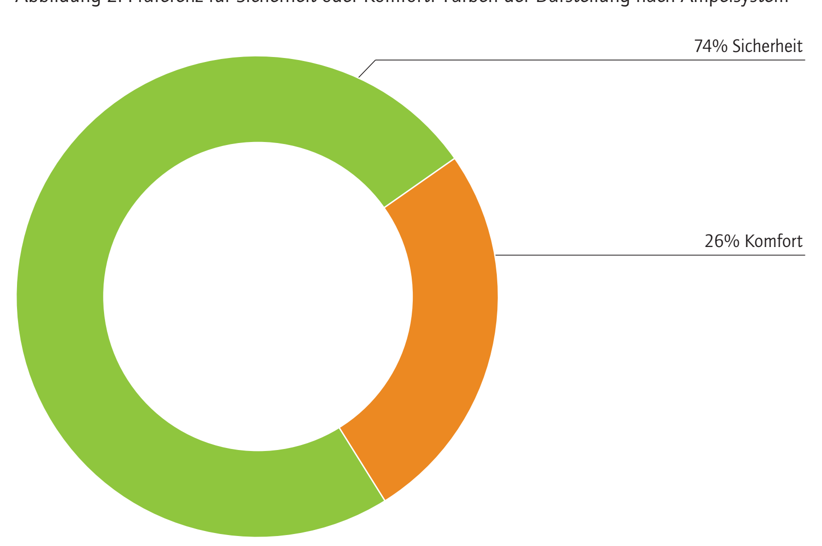


Antworten auf Fragen nach Gefährdungspotenzial von Technologien und Anwendungen zeigen, dass Bedrohungen im privaten Umfeld konkret verortet werden: die Top-Positionen problematischer Alltagsanwendungen werden von Online-Banking und E-Mail besetzt und beim Technologie-Ranking hinsichtlich Gefährdungspotenzial führt WLAN als Risiko-Technologie deutlich vor (jeweils auf gleichem Rang) mobilen Geräten und Datenträgern (zum Beispiel USB-Sticks oder externen Festplatten) sowie VOIP. Noch eindeutiger als für das Privatumfeld fällt das Urteil für den Unternehmensbereich aus: 96 Prozent halten das Thema in diesem Kontext für „sehr wichtig", Nennungen unterhalb von „wichtig" belaufen sich insgesamt unter 1 Prozent.

Den positiven Eindruck im Hinblick auf Sensibilisierung rundet ein letztes Ergebnis ab: „Wenn Sie bei der Computernutzung zwischen Komfort und Sicherheit wählen müssten, was wäre Ihnen wichtiger?" So lautet eine Frage, auf die fast drei Viertel aller zukünftigen IT-Entscheider angeben, der Sicherheit den Vorzug vor dem Komfort zu geben (siehe Abbildung 2).

Abbildung 2: Präferenz für Sicherheit oder Komfort? Farben der Darstellung nach Ampelsystem











4.3.2 REALISTISCHE BEWERTUNG DES STUDENTISCHEN SELBSTBILDES

Die Studierenden erkennen die hohe Bedeutung des Aspekts Sicherheit, befassen sich auch unabhängig von ihrem Studium mit dem Thema und stellen den Komfort zurück, wenn er die Sicherheit gefährden könnte – so das bisherige Fazit. Gibt es Hinweise darauf, dass dieses positive Bild der Realität nahekommt oder ihr eher widerspricht?

Ein erstes Indiz ergibt sich im Hinblick auf die IT-Sicherheitskompetenz. Bei einer Reihe von Fragen, die sich mit dem Risikopotenzial verschiedener Technologien und Anwendungen beschäftigen, besteht die Möglichkeit, anzugeben, ein genanntes Stichwort nicht zu kennen (bzw. nicht zu verstehen). Hier zeigt sich, dass die Begriffe „Denial of Service-Attacken" und „Pharming" immerhin etwa zwanzig Prozent der Antwortenden nicht bekannt sind. Bei den Maßnahmen gegen Gefährdungen ist der Spitzenreiter im Hinblick auf unbekannte Vorgaben „Verschlüsselung auf mobilen Datenträgern/Geräten" auf einem Niveau von immerhin noch ca. sechs Prozent der Antworten.

Die entscheidende Erkenntnis liefert allerdings die Frage nach den persönlich verwendeten Sicherheitsmaßnahmen (siehe Abbildung 3). Hier zeigt sich, dass nur Antiviren-Software, Firewall und (mit Einschränkungen) die regelmäßige Aktualisierung von Software sowie das Löschen von Cookies und Cache zu den Standardmaßnahmen gezählt werden können.



Abbildung 3: Eigene Verwendung von Sicherheitsmaßnahmen. Farben der Darstellung nach Ampelsystem



Obwohl immerhin fast drei Viertel aller Befragten (72 Prozent) über eigene Erfahrungen mit Datenverlust berichten, wird Datensicherung – eine wirklich sehr einfache Maßnahme – offensichtlich nur eher unsystematisch betrieben. Auch Passwörter werden von fast 40 Prozent der Befragten höchstens selten geändert.

Das Signieren von E-Mails bzw. das Verschlüsseln von E-Mails oder von Daten auf mobilen Datenträgern haben sich in keiner Weise breit eingeführt: Fast fünfzig Prozent geben an, diese Techniken noch nie eingesetzt zu haben!

Zusammenfassend muss also der im Hinblick auf Awareness und Sensibilisierung sehr positive Eindruck deutlich relativiert werden. Die Studierenden genügen offensichtlich, was ihr tatsächliches Verhalten betrifft, ihrem eigenen Anspruch nicht – und der Lernort Hochschule macht sie offensichtlich auch nicht mit den fortgeschrittenen Techniken für IT-Sicherheit vertraut, obwohl dort viele sensible Anwendungen betrieben und sicherheitsrelevante Online-Dienstleistungen angeboten werden.

4.4 IT-SICHERHEIT ALS THEMA IM STUDIUM



Die GI-Empfehlungen „IT-Sicherheit in der Ausbildung“ aus dem Jahr 2006 lauten wie folgt: „[...] Grundlagen der IT-Sicherheit [sollen] für alle Studierenden unabhängig von ihrer Fachrichtung Bestandteil der akademischen Ausbildung sein. Besonders in Informatik- bzw. informatiknahen Bachelor- und Master-Studiengängen [...] muss Sicherheit ein Bestandteil des Curriculums sein und je nach individuellem Interessenschwerpunkt in Wahlpflichtveranstaltungen vertieft werden können.“[5] Ausdrücklich wird für alle Studiengänge, unabhängig vom speziellen Fach, gefordert: „Ziel der Ausbildung in allen Studiengängen, auch in jenen ohne direkten Informatikbezug, muss die Bewusstseinsbildung um die möglichen Risiken und Gefahren der IT-Nutzung und die Vermittlung von Wissen über entsprechende Schutzmechanismen sein. IT-Sicherheit muss in allen Studiengängen als Querschnittsthema mit Anwendungsbezug Berücksichtigung finden.“[6] Die Untersuchung geht nun der Frage nach, inwieweit diese Forderungen zu Studiengängen und deren Ausgestaltung geführt haben, die von den Studierenden der Informatik bzw. informatiknaher Studiengänge entsprechend wahrgenommen werden.

Zunächst ist wieder die Frage nach der Selbsteinschätzung zu stellen: Wie wichtig ist den Studierenden das Thema „IT-Sicherheit“ in ihrem Studium? 40 Prozent antworten insgesamt mit „wichtig“ oder „sehr wichtig“; keine 6 Prozent geben „unwichtig“ oder „sehr unwichtig“ an. Der Informatikanteil am Studium ist dabei Einflussgröße: Je höher der Informatikstudienanteil, desto häufiger erfolgt die Nennung „sehr wichtig“. Je geringer der Informatikstudienanteil, desto häufiger ist auch eine neutrale Einschätzung der Bedeutung von IT-Sicherheit im Studium.

---

[5] GI 2006, S. 2.
[6] GI 2006, S. 4.





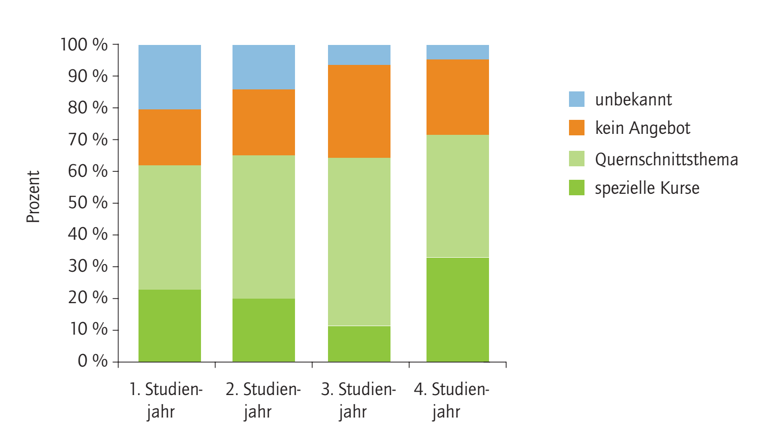
Beim Lehrangebot der Hochschulen zum Thema „IT-Sicherheit" ergibt sich ein kritisches Bild: Rechnet man die Antworten der Personen heraus, die sich kein Urteil zutrauen, so erklären knapp 25 Prozent, dass das Thema „IT-Sicherheit" in Lehrveranstaltungen nicht vorkommt. Dies sind nur vier Prozent weniger als der Anteil der Personen, die angeben, dass es spezielle Kurse zur IT-Sicherheit gibt. Knapp die Hälfte (46 Prozent) sagt, dass das Thema „IT-Sicherheit" im Rahmen anderer Kurse angesprochen wird.

Da die Wahrnehmung des Lehrangebotes stark davon abhängig ist, wie lange man bereits studiert, wird der Einfluss des Studienfortschritts genauer untersucht. Abbildung 4 zeigt die Differenzierung der Antworten nach Studienjahren. Plausiblerweise nimmt die Zahl derjenigen, die sich über das Lehrangebot kein Urteil erlauben wollen, mit zunehmendem Studienfortschritt ab. Bei der Frage nach den speziellen Kursen gibt es nicht wirklich einen Trend; allerdings stammt hier die höchste Angabe mit ca. 35 Prozent von Studierenden ab dem vierten Studienjahr. Überraschenderweise ist die Anzahl derjenigen, die „kein Lehrangebot" konstatieren, nach dem zweiten Studienjahr größer. Es gibt zwei mögliche Erklärungen: Entweder sind Studierende höherer Semester anspruchsvoller und kritischer oder aber Lehrveranstaltungen, die inzwischen in ersten Semestern angeboten werden, sind erst neuesten Datums.





Abbildung 4: Verfügbares Lehrangebot, differenziert nach Studienfortschritt. Farben der Darstellung nach Ampelsystem



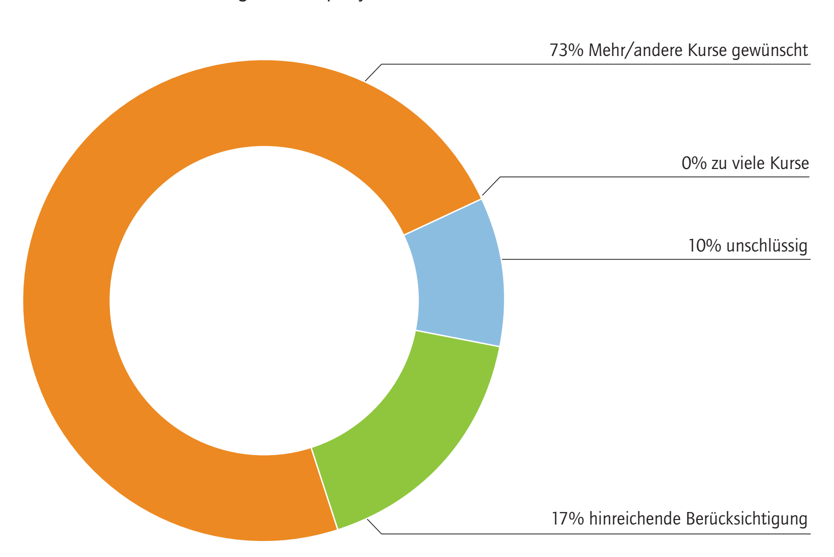


Die Frage nach dem Umfang des Lehrangebots ist zunächst nicht wertend. Nach einer solchen Wertung werden zusätzlich die zukünftigen IT-Entscheider folgendermaßen gefragt: „Werden Sie, nach Ihrer heutigen Einschätzung, durch das Studium angemessen auf das Thema IT-Sicherheit für Ihren zukünftigen Beruf vorbereitet?" Die Antworten zeigen, dass hier die Studierenden einen dramatischen Handlungsbedarf sehen: Nur 18 Prozent glauben, dass das Thema hinreichend im Studium berücksichtigt wird. Die große Mehrheit (61 Prozent) wünscht sich mehr bzw. andere Lehrveranstaltungen zum Thema „IT-Sicherheit". Dass Studierende der ersten Studienjahre sich vielfach noch kein Urteil zutrauen, spricht für deren Realismus. Aus diesem Grund zeigt Abbildung 5 die Auswertung für die Studierenden ab dem zweiten Studienjahr: Bei nur zehn Prozent Enthaltungen wünschen sich fast drei Viertel ein größeres und anderes Lehrangebot!





Abbildung 5: Urteil nach zwei Jahren Studium: Angemessene Vorbereitung auf den Beruf durch das Studium? Farben der Darstellung nach Ampelsystem







In Abschnitt 4.3.1 wird dokumentiert, dass die meisten Befragten angeben, sich entweder umfassend oder zumindest partiell mit dem Thema „IT-Sicherheit" beschäftigt zu haben. Diese Beschäftigung muss aber keineswegs im Rahmen von Lehrveranstaltungen erfolgt sein. Die Frage danach, in welchem Umfang schon Lehrveranstaltungen zum Thema „IT-Sicherheit" besucht wurden, ergibt einen Befund, den (nach Studienfortschritt aufgeschlüsselt) Abbildung 6 zeigt. Die Antwortalternativen sind:

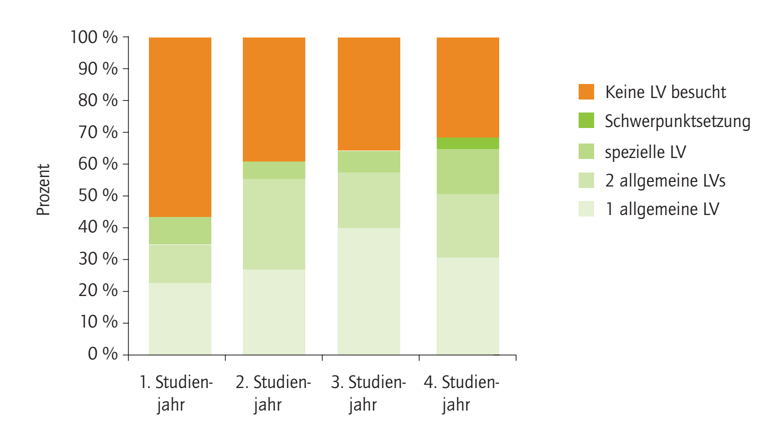
- „Ich habe noch keine Lehrveranstaltung mit dieser Thematik besucht";
- „Ich habe bis jetzt nur eine Lehrveranstaltung besucht, die das Thema u. a. angesprochen hat";
- „Ich habe bis jetzt mehrere Lehrveranstaltungen besucht, die das Thema angesprochen haben";
- „Ich habe bis jetzt eine spezielle Lehrveranstaltung zum Thema besucht";
- „Ich habe meinen Schwerpunkt auf das Thema gelegt".

Man erkennt plausible Trends: Mit zunehmendem Studienfortschritt sinkt die Zahl derjenigen, die noch keine Lehrveranstaltung besucht haben, und es wächst die Anzahl der Hörer spezieller Lehrveranstaltungen. Allerdings zeigt die Auswertung: Über sechzig Prozent aller Studierenden, die sich im vierten Studiensemester (oder in höheren Studiensemestern) befinden, haben im Verlauf ihres bisherigen Studiums insgesamt höchstens an einer (einzigen) Lehrveranstaltung teilgenommen, die das Thema unter anderem anspricht!





Abbildung 6: Besuch von Lehrveranstaltungen über IT-Sicherheit, differenziert nach Studienjahr. Farben der Darstellung nach Ampelsystem







Fazit zum Thema „Hochschulausbildung“: Die Studierenden halten das Thema „IT-Sicherheit“ im Studium für (mindestens) wichtig und sind mit dem Lehrangebot der Hochschulen zu diesem Thema massiv unzufrieden. Knapp drei Viertel aller Studierenden nach dem zweiten Studienjahr (dem vierten Semester!) geben an, dass sie sich mehr oder andere Lehrveranstaltungen zum Thema der IT-Sicherheit wünschen. Selbst nach dem dritten Studienjahr haben weit mehr als die Hälfte (62 Prozent) nicht mehr als eine einzige Lehrveranstaltung besucht, in der IT-Sicherheit „unter anderem angesprochen wird“.

4.5 VERANTWORTUNG DER AKTEURE IM HINBLICK AUF IT-SICHERHEIT

Abschließend gibt die Studie auch eine Einschätzung, wie zukünftige IT-Entscheider das Thema der IT-Sicherheit im gesellschaftlichen Kontext einschätzen, wer die relevanten Akteure sind und wie diese ihrer Verantwortung – nach Einschätzung der Befragten – gerecht werden.

Wenn es um die sichere Nutzung von Informationstechnologie und Internet geht, sind nach Ansicht der Studierenden „sehr stark“ gefordert die Nutzer (63 Prozent), die Anbieter (56 Prozent), die Hochschulen und Schulen (37 Prozent) und die Politik (26 Prozent). Als hauptsächlich „stark“ gefordert werden Fachgesellschaften und Verbände, Medien und Verbraucherverbände weitgehend mit gleichen Anteilen genannt.





Kaum einem der genannten Akteure wird bescheinigt, das Thema „IT-Sicherheit“ ausreichend zu berücksichtigen. Ausschließlich den Fachgesellschaften und Verbänden gelingt es, mit 52 zu 48 Prozent eine knapp positive Bilanz der Ja- und Nein-Antworten zu erreichen. Deutlich negativ wird diese Bilanz bereits bei den Hochschulen und Schulen (44 zu 56 Prozent) und Anbietern (42 zu 58 Prozent). Alle übrigen Fälle werden noch deutlich ungünstiger beurteilt. Schlusslichter sind die Politik (20 zu 80 Prozent) und die Nutzer (15 zu 85 Prozent).

4.5.1 DIE POLITIK IN DER EINSCHÄTZUNG ZUKÜNFTIGER IT-ENTSCHEIDER

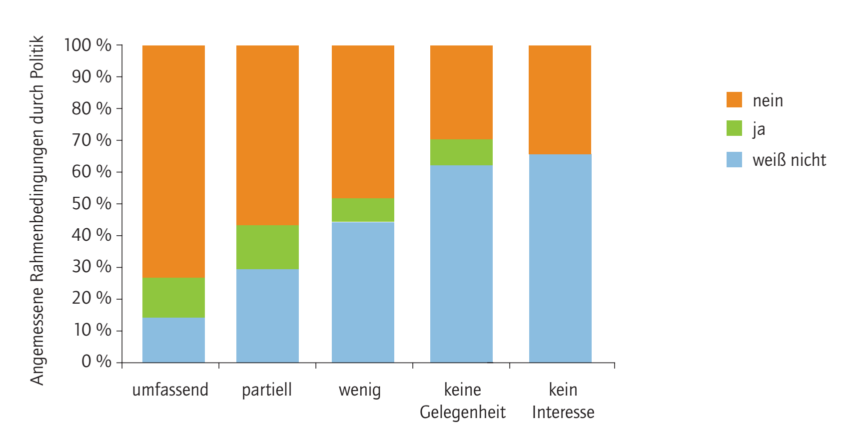
Die Politik liegt im Mittelfeld derer, die nach Einschätzung der Studierenden im Hinblick auf die sichere Nutzung von Informationstechnologien und Internet „stark“ oder „sehr stark“ gefordert sind. Achzig Prozent sind der Meinung, dass das Thema „IT-Sicherheit“ von der Politik nicht ausreichend berücksichtigt wird.

Weitergehend wurden die zukünftigen IT-Entscheider nun gefragt, ob von der Politik angemessene Rahmenbedingungen für die Probleme der IT-Sicherheit geschaffen wurden bzw. geschaffen sind. 81 Prozent derjenigen, die sich ein Urteil zutrauen, meinen „nein“! Diese Antworten zeigt Abbildung 7 aufgeschlüsselt danach, inwieweit sie von Personen stammen, die sich tatsächlich für kompetent halten. Die Auswertung zeigt, dass das Urteil der zukünftigen IT-Entscheider durchaus ernst genommen werden sollte: Je mehr sich die Befragten mit der Problematik von IT-Sicherheit beschäftigt ha-



ben, desto größer ist der Anteil derer, die die politischen Rahmenbedingungen negativ beurteilen. Ebenso sinkt der Anteil derjenigen, die sich kein Urteil zutrauen. Besonders eindeutig negativ ist das Urteil bei denjenigen, die sich umfassend mit IT-Sicherheit beschäftigt haben.

Abbildung 7: Beurteilung politischer Rahmenbedingungen in Abhängigkeit von eigener Kompetenz. Farben der Darstellung nach Ampelsystem






Fazit zum Thema „IT-Sicherheit" im gesellschaftlichen Kontext: Nach Meinung zukünftiger IT-Entscheider sind es einerseits die Nutzer, die am stärksten gefordert sind, wenn es um die sichere Nutzung von Informationstechnologien und Internet geht, und es sind auch die Nutzer, denen am weitgehendsten attestiert wird, dass sie das Thema „IT-Sicherheit" nicht ausreichend berücksichtigen.

Der Politik wird zu über achzig Prozent bescheinigt, dass sie für die Probleme der IT-Sicherheit keine angemessenen Rahmenbedingungen geschaffen hat. Dabei ist diese negative Einschätzung für die Politik umso stabiler, je mehr sich die Befragten bereits mit dem Thema „IT-Sicherheit" beschäftigt haben.





4.6 LITERATUR

GI 2001
Gesellschaft für Informatik e.V.: IT-Sicherheit essenziell für E-Everything. GI und DECUS fordern verstärkte Ausbildung von Fachleuten. Pressemitteilung 15. November 2001. URL: http://www.gi-ev.de/presse/pressemitteilungen-thematisch/pressemitteilung-vom-15-november-2001.html [Stand: 22.7.2009].

GI 2006
Gesellschaft für Informatik e.V.: IT-Sicherheit in der Ausbildung. Empfehlung zur Berücksichtigung der IT-Sicherheit in der schulischen und akademischen Ausbildung. URL: http://www.gi-ev.de/fileadmin/redaktion/empfehlungen/GI-Empfehlung-IT-Sicherheit-in-der-Ausbildung-2006.pdf [Stand: 22.7.2009].

Knorz 2008
Knorz. G.: Studie zur IT-Sicherheit. Einstellungen und Einschätzungen zukünftiger Entscheider. URL: http://www.h-da.de/fileadmin/documents/Publikationen/Studie-IT-Sicherheit-V1-0.pdf [Stand: 22.7.2009].









> ZUR UMSETZUNG VON SICHERHEIT IN DER PRAXIS





1 „FORSCHUNG FÜR DIE ZIVILE SICHERHEIT" – DAS NATIONALE SICHERHEITSFORSCHUNGS-PROGRAMM

ANDREAS HOFFKNECHT/OLAV TEICHERT/AXEL ZWECK

1.1 EINLEITUNG

Der Erfolg unserer exportorientierten Wirtschaft ist ohne den freien Informations-, Personen- und Warenverkehr undenkbar. Sichere Energie- und Verkehrsnetze, Internet und Telekommunikation, Lebensmittel- und Gesundheitsversorgung sind die Lebensnerven unserer hochgradig vernetzten Gesellschaft. Aber auch Sicherheitsrisiken haben sich gewandelt. Terrorismus und extremistische Angriffe, die Verbreitung von Massenvernichtungswaffen, regionale Konflikte, der Zusammenbruch von Staaten, die organisierte Kriminalität sowie Natur- und Umweltkatastrophen stellen auch für Deutschland ein großes Gefährdungspotenzial dar. Gefahren und Bedrohungen können dabei sehr vielfältig und unterschiedlich in ihrer Wirkung sein, den Einzelnen oder die gesamte Gesellschaft betreffen. Auch ohne Terror können aus kleinen Ursachen große negative Wirkungen erwachsen. Bekannte Beispiele sind der Sturm Kyrill, der den Verkehr in Deutschland lahmlegte, oder der europaweite Stromausfall, nachdem ein Kabel an der Ems getrennt wurde. Deutschlands hocheffiziente, automatisierte und vernetzte Infrastrukturen reagieren sehr sensibel auf Eingriffe.

Zur Verbesserung des Schutzes der Bürgerinnen und Bürger hat das Bundesministerium für Bildung und Forschung im Jahr 2007 das Programm der Bundesregierung „Forschung für die zivile Sicherheit" gestartet. Das Sicherheitsforschungsprogramm bildet einen zentralen Schwerpunkt in der nationalen Hightech-Strategie.[1] Vorrangiges Ziel ziviler Sicherheitsforschung ist es, mit der Entwicklung innovativer Lösungen die zivile Sicherheit der Bürgerinnen und Bürger zu erhöhen und die Balance zwischen Sicherheit und Freiheit zu wahren. Das Sicherheitsforschungsprogramm verknüpft dabei Geistes- und Sozialwissenschaften mit den Natur- und Technikdisziplinen, die gemeinsam innovative Sicherheitslösungen erarbeiten. Dafür stellt das Bundesministerium für Bildung und Forschung in der ersten Förderperiode bis zum Jahr 2010 Haushaltsmittel im Umfang von mehr als 123 Millionen Euro zur Verfügung.

[1] Siehe auch http://www.bmbf.de/de/6608.php.





1.2 STRATEGISCHE ZIELE

Ausrichtung auf den Bedarf der Endnutzer: Mit seiner bedarfsorientierten und interdisziplinären Ausrichtung ist das Sicherheitsforschungsprogramm bewusst als offenes und lernendes Forschungsprogramm ausgelegt. So sind, um dem Bedarf an Sicherheit möglichst präzise und schnell gerecht werden zu können, die Endnutzer als „Kunden" unmittelbar in die Durchführung der Projekte eingebunden. Endnutzer sind Behörden und Organisationen mit Sicherheitsausgaben (zum Beispiel Polizei, Technisches Hilfswerk, Feuerwehr, Gesundheitsämter), Bundesbehörden wie die Bundesanstalt für Straßenwesen sowie staatliche und private Betreiber kritischer Infrastrukturen (Bahn, Energie- und Gesundheitssektor, Telekommunikation, öffentlicher Nahverkehr, Flughäfen, Logistik und anderes). Da sich etwa 80 Prozent aller sicherheitsrelevanten Infrastrukturen in einer privatwirtschaftlichen Trägerschaft befinden, werden mit diesem Programm Anreize geschaffen, dass Staat und Privatwirtschaft Hand in Hand arbeiten, um Zielkonflikte bei der Implementierung neuer Sicherheitslösungen frühzeitig zu minimieren.

Die Kooperation mit allen Bundesressorts ist integraler Bestandteil des Programms. Das Wirtschaftsressort, das Verkehrs- und das Gesundheitsministerium sowie insbesondere das Bundesministerium des Inneren sind zentrale Akteure der Sicherheitsforschung. Hier wirkt der ressortübergreifende Ansatz der Hightech-Strategie in besonderer Weise.




Marktorientierung: Neben dem Schutz vor Gefahren und der Schaffung sicherer Standortbedingungen bieten sicherheitstechnische Produkte und Dienstleistungen große Chancen für die Wirtschaft. Allein im Jahr 2008 betrug laut einer vom Bundesministerium für Wirtschaft und Technologie in Auftrag gegebenen Studie das Marktvolumen sicherheitstechnischer Produkte und Dienstleistungen in Deutschland rund 20 Milliarden Euro. Die jährlichen Wachstumsraten sind hoch – laut OECD liegen sie weltweit bei rund sieben Prozent im Jahr. Damit bieten Sicherheitstechnologien internationale Wettbewerbsvorteile und entwickeln sich zu einem wichtigen Leitmarkt. Der Staat als Nachfrager im Bereich Sicherheitslösungen eröffnet dabei neue Marktmöglichkeiten und erleichtert die Einführung neuer Technologien. Nicht zuletzt schafft die steigende Nachfrage nach sicherheitsrelevanten Produkten und Dienstleistungen Werte und neue Arbeitsplätze und stärkt so die Wettbewerbsfähigkeit der deutschen Wirtschaft.

Disziplinübergreifende Zusammenarbeit: Sicherheitstechnologien sind Querschnittstechnologien, die Beiträge unterschiedlicher Disziplinen der Technik- und Naturwissenschaften erfordern. Sicherheit ist aber nicht allein mit Technologien erreichbar; sie hängt immer auch vom Handeln der Menschen ab. Das Sicherheitsforschungsprogramm ist deshalb kein reines Technologieprogramm und fördert nicht nur die Entwicklung technischer Neuerungen, sondern ausdrücklich auch innovative organisatorische Konzepte und Handlungsstrategien. Interdisziplinäre Projekte mit Beteiligung der Geistes- und Sozialwissenschaften, Wissenstransfer in die Öffentlichkeit, Begleitforschung zu kritischen





Fragen und Transparenz sind integraler Bestandteil und werden von allen Akteuren als wesentliche Voraussetzung für den Erfolg des Sicherheitsforschungsprogramms angesehen.

Vernetzung der Akteure: Das nationale Sicherheitsforschungsprogramm eröffnet die Möglichkeit, durch Forschung und Innovation die Wettbewerbsfähigkeit aller Unternehmen, die Beiträge zur Sicherheit erbringen, zu stärken und die Technologieführerschaft in spezifischen Sicherheitstechnologien zu erreichen. Es gilt, Sicherheit als nationalen Standort- und Wirtschaftsfaktor zu etablieren und Gestaltungsspielräume auf europäischer Ebene zu eröffnen. Das Sicherheitsforschungsprogramm bietet hierzu eine wichtige Plattform, auf der Industrie, Forschungseinrichtungen und Hochschulen mit Behörden, Rettungs- und Sicherheitskräften sowie den Betreibern von Energie-, Verkehrs-, Lebensmitteln und Gesundheitsversorgung zusammenarbeiten können.

Das Bundesministerium für Bildung und Forschung unterstützt die Vernetzung aller Akteure in der zivilen Sicherheitsforschung in Deutschland auf vielfältige Weise. Auf der interaktiven Forschungslandkarte „SecurityResearchMap“[2] präsentieren sich bereits über 280 deutsche, in der Sicherheitsforschung aktive Institutionen mit ihren Profilen; sie sind nach verschiedenen Kriterien – von den thematischen Schwerpunkten über die geografische Lage der Institution bis hin zur Volltextsuche – recherchierbar.



Mit dem im Rahmen der Hightech-Strategie neu geschaffenen Instrument der Innovationsplattformen[3] unterstützt das Bundesministerium für Bildung und Forschung den Aufbau strategischer Partnerschaften. Die Innovationsplattformen bieten allen interessierten Akteuren aus Forschung, Industrie, den Behörden und Organisationen mit Sicherheitsaufgaben und weiteren zuständigen Bundes- und Landesressorts bzw. deren nachgeordneten Bereichen ein Forum für den kontinuierlichen Dialog.

Europäische Zusammenarbeit und internationale Forschungsallianzen: Zivile Sicherheitsforschung kann nur im internationalen, mindestens im europäischen Kontext wirksam erfolgen. Internationale Forschungsallianzen, die europäische Forschungszusammenarbeit und die Mitgestaltung der europäischen Sicherheitsarchitektur sind deshalb weitere Ziele des Sicherheitsforschungsprogramms. Auch die Europäische Union hat diese Herausforderungen angenommen und innerhalb des 7. Forschungsrahmenprogramms ein eigenes Sicherheitsforschungsprogramm aufgelegt, das einen wichtigen Grundstein für die EU-Zusammenarbeit in der zivilen Sicherheitsforschung gelegt hat. Die enge Verzahnung mit dem europäischen Sicherheitsforschungsprogramm und den entsprechenden Politikbereichen untermauert die starke Rolle Deutschlands beim Aufbau einer europäischen Sicherheitsarchitektur.

Gesellschaftlicher Dialog: Der Dialog zwischen den verschiedenen gesellschaftlichen Akteuren – von der Wissenschaft über Industrie und Endnutzer bis zu den Bürgerinnen und Bürgern – ist ein wichtiger Bestandteil des Sicherheitsforschungsprogramms.

---

2 Vgl. auch http://www.securityresearchmap.de/cgi-bin/sifomap.pl.
3 Vgl. auch http://www.bmbf.de/de/12907.php.





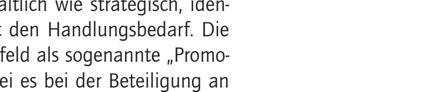
Er soll wesentlich zu einem besseren Verständnis der Herausforderungen und zu einer transparenten Darstellung der Forschungsthemen in der Öffentlichkeit beitragen und ist damit ein entscheidender Erfolgsfaktor des Sicherheitsforschungsprogramms.

1.3 UMSETZUNG DES SICHERHEITSFORSCHUNGSPROGRAMMS

Bei der Umsetzung des Programms „Forschung für die zivile Sicherheit" ist auf eine systematische Einbindung aller für die zivile Sicherheitsforschung relevanten Akteure und zuständigen Ressorts geachtet worden. Deshalb ist auf programmatischer Ebene ein Wissenschaftlicher Programmausschuss[4] verankert worden, der als unabhängiges Expertengremium die Bundesregierung in Fragen der Sicherheitsforschung berät. Darüber hinaus wird das Sicherheitsforschungsprogramm auf der übergeordneten Ebene der Hightech-Strategie durch die Forschungsunion Wirtschaft – Wissenschaft[5] intensiv begleitet. Bereits in dem ersten, 2007 veröffentlichten Fortschrittsbericht unterstützte die Forschungsunion ausdrücklich die im Programm vorgenommene Schwerpunktsetzung. Bekräftigt wurde der im Sicherheitsforschungsprogramm eingeschlagene Weg in den jüngst im Rahmen der Hightech-Strategie-Konferenz[6] am 6. Mai 2009 von der Forschungsunion vorgestellten Empfehlungen „Woher das neue Wachstum kommt". Dabei wurde „Sicherheit 2020" als eines von fünf prioritären Bedarfsfeldern der zukünftigen Forschungsförderung in der Hightech-Strategie identifiziert und gleichzeitig die Empfehlung ausgesprochen, sich in den Bedarfsfeldern noch stärker auf leitmarktorientierte, an Wertschöpfungsketten ausgerichtete Programme zu konzentrieren.



Die Förderstrukturen des Sicherheitsforschungsprogramms konzentrieren sich auf unterschiedliche Programmlinien. Programmlinie 1 umfasst die „Szenarienorientierte Sicherheitsforschung". In dieser Programmlinie wird die Forschung auf Lösungen für komplexe Sicherheitsszenarien fokussiert. Damit wird die Problemlösungsperspektive der Endnutzer und Anwender von Beginn an in die Forschung eingebracht und ist unter anderem auf die Verbesserung der Zusammenarbeit zwischen Behörden und privaten Betreibern sicherheitsrelevanter Infrastrukturen angelegt. Die Szenarienorientierung



4 Der Wissenschaftliche Programmausschuss zur Sicherheitsforschung hat sich am 29.10.2007 in Bonn konstituiert. Ihm gehören Persönlichkeiten aus den Bereichen Forschung, Wissenschaft, Behörden und Unternehmen an. Im Mittelpunkt der Beratung und Unterstützung stehen die inhaltliche Ausrichtung und Zielorientierung der Sicherheitsforschung (zum Beispiel im Rahmen der Programmevaluierung), Empfehlungen für den Wissenstransfer in die Praxis sowie Unterstützung und Begleitung einer Verzahnung der deutschen mit den europäischen Aktivitäten (vgl. http://www.bmbf.de/de/11781.php).

5 In der Forschungsunion Wirtschaft – Wissenschaft arbeiten Experten aus Wirtschaft, Wissenschaft und Politik auf hoher Ebene zusammen. Sie begleitet die Hightech-Strategie inhaltlich wie strategisch, identifiziert Innovationshemmnisse, formuliert Forschungsaufgaben und benennt den Handlungsbedarf. Die Mitglieder der Forschungsunion wirken in ihren Einrichtungen und ihrem Umfeld als sogenannte „Promotoren" der einzelnen Innovationsfelder und unterstützen deren Umsetzung, sei es bei der Beteiligung an Innovationsallianzen oder als Botschafter für den FuE-Standort Deutschland (siehe auch BMBF 2007a).

6 Siehe auch http://www.hightech-strategie.de/de/984.php.





stellt sicher, dass isolierte Einzelfragen und Einzellösungen zugunsten passfähiger Systeminnovationen vermieden werden. Diese Systeminnovationen integrieren bestehende und neue Technologien. Sie stützen sich auf Bedrohungsanalysen und berücksichtigen Kosten-Nutzen-Analysen ebenso wie die Einstellungen und das Verhalten von Einzelnen oder Gruppen und deren Dynamik: Wie können Bürgerinnen und Bürger in Krisensituationen zur Reduzierung oder Vermeidung von Gefahrenpotenzialen besser beitragen? Wie kann Fehlverhalten, zum Beispiel in Paniksituationen, vermieden werden? Indem sie diesen Fragen nachgeht, wird die szenarienorientierte Sicherheitsforschung dem tatsächlichen Sicherheitsbedarf gerecht und zugleich auf eine rasche Umsetzung der Ergebnisse in die Praxis ausgerichtet. Kernthemen der Förderung sind: Schutz und Rettung von Menschen, Schutz von Verkehrsinfrastrukturen, Schutz vor Ausfall von Versorgungsinfrastrukturen sowie Sicherung der Warenketten.

Programmlinie 2 zielt auf die Erforschung von Querschnittstechnologien in „Technologieverbünden“ ab, die in vielen Szenarien benötigt werden. Dazu zählen Technologien zur raschen und mobilen Erkennung von Gefahrstoffen, zur Einsatzertüchtigung von Sicherheits- und Rettungskräften, zur Mustererkennung und zur schnellen und sicheren Personenidentifikation. Die Technologieverbünde erschließen für die Sicherheitsforschung wichtiges Basiswissen und entwickeln aus bestehenden und neuen Technologien innovative Systeme. Durch Einbeziehung der gesamten Innovationskette von der Forschung über die Industrie bis hin zu den Endnutzern arbeiten sie anwendungsnah.





Neben den genannten beiden Programmlinien, in denen technische und gesellschaftliche Fragestellungen integriert bearbeitet werden, werden in einer eigenen Förderlinie gesellschaftliche Querschnitts- und Grundsatzfragen adressiert.

Das Programm setzt auf eine an Wettbewerb und Transparenz orientierte, breite und innovative Sicherheitsforschung. Die Fördermittel werden deshalb auf Basis von Ausschreibungen, also des Wettbewerbs um den besten Ansatz vergeben. Unternehmen beteiligen sich mit 50 Prozent bzw. 40 Prozent bei kleineren und mittleren Unternehmen (KMU) an den Kosten.





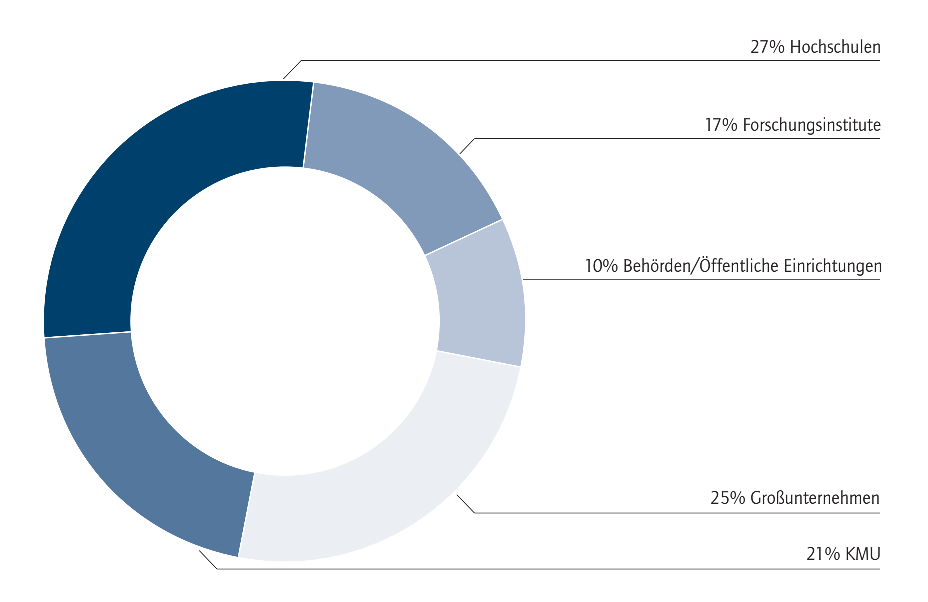
1.3.1 AKTUELLER STAND DER FÖRDERUNG

Gut zwei Jahre nach Start des Programms befinden sich 49 Verbundprojekte aus den ersten vier Bekanntmachungen in der Förderung. Weitere Förderschwerpunkte befinden sich in der Vorbereitung.

Abbildung 1 zeigt einen Zwischenstand zur Verteilung der aktuell 303 Zuwendungsempfänger. Erfreulich ist der hohe KMU-Anteil von insgesamt 21 Prozent, entsprechend einem Anteil von 46 Prozent aller beteiligten Unternehmen. Davon engagieren sich 45 Prozent erstmalig in einem vom Bundesministerium für Bildung und Forschung geförderten Verbundprojekt. In die Verbundprojekte sind öffentliche bzw. private Endnutzer, entweder als direkte Zuwendungsempfänger oder als Unterauftragnehmer bzw. assoziierte Partner eingebunden.

Abbildung 1: Verteilung der bisher geförderten 303 Zuwendungsempfänger auf die verschiedenen Institutionen. Die Verteilung gibt lediglich eine Zwischenbilanz auf Basis der Projekte wieder, die bis Ende Juni 2009 bewilligt waren.







Das Schwerpunktthema „Schutz von Verkehrsinfrastrukturen" zielt auf den Schutz sämtlicher Transportwege und bezieht auch dazugehörige Einrichtungen wie Flughäfen, Bahnhöfe und U-Bahn-Systeme oder Brücken und Tunnel mit ein. Die Forschungsthemen sind so vielfältig wie die zugrunde liegenden Infrastrukturen. Einen Förderschwerpunkt bildet die Integration von Sensoren in Brücken- oder Tunnelelemente, die kontinuierlich





sowie bei einem Schadensereignis den Zustand des Bauwerks an eine Rettungsleitstelle übermitteln. Einen weiteren Förderschwerpunkt bildet die Entwicklung effektiver Sicherheitsmaßnahmen im öffentlichen Personennahverkehr. Beispielsweise werden hier voraussichtliche Kontaminationsverläufe bei der Freisetzung gefährlicher Stoffe innerhalb eines U-Bahn-Systems untersucht. Die Schulung von Mitarbeitern und Mitarbeiterinnen der Verkehrsunternehmen stellt einen weiteren wichtigen Aspekt dar. Die Mitarbeiter sollen dazu befähigt werden, Gefahren im Voraus zu erkennen und angemessen zu reagieren.

In der maritimen Sicherheitsforschung liegt der Forschungsschwerpunkt auf dem Schutz der Personen- und Frachtschifffahrt. Untersucht werden sowohl organisatorische als auch technologische Fragen, die die Entwicklung neuer Kontroll- und Überwachungssysteme einschließen. Ein Ziel der Forschung zur Flughafensicherheit ist es, Kontrollprozeduren kundenfreundlich, effizient, barrierefreier sowie kostengünstiger zu gestalten und gleichzeitig ein Maximum an Sicherheit zu gewährleisten. Dabei soll schon im Vorfeld der Implementierung neuer oder angepasster Sicherheitsmaßnahmen untersucht werden, wie diese von Fluggästen und Flughafenmitarbeitern angenommen werden.




Beim Forschungsschwerpunkt „Schutz und Rettung von Menschen“ stehen unter anderem Alltagssituationen wie Großveranstaltungen im Blickpunkt, bei denen durch den Eintritt katastrophaler Ereignisse komplexe Krisensituationen bzw. Großschadensereignisse entstehen können. Eine zentrale Fragestellung ist, wie unterschiedliche Daten – zum Beispiel eines Gebäudemanagementsystems – zu Rauch- und Hitzeentwicklung oder auch zu Notausgängen in Echtzeit in Evakuierungsprozesse eingebunden und über mobile Endgeräte entsprechende Lageinformationen den Einsatzkräften vor Ort zur Verfügung gestellt werden können. Ein Teil der Verbundprojekte beschäftigt sich auch mit der Optimierung der Verletztenversorgung in Katastrophenfällen. Ziel ist ein mobiles Informations- und Kommunikationssystem, das allen Personen, die an der Rettung bzw. Bergung, am Transport und an der Unterbringung der Betroffenen in Krankenhäusern beteiligt sind, zur Verfügung steht. Weitere Projekte aus den szenarioorientierten Schwerpunktthemen „Schutz vor Ausfall von Versorgungsinfrastrukturen“ und „Sicherung von Warenketten“ befinden sich derzeit in der Antragsphase.

In der Projektlinie 2 („Technologieverbünde“) sind 25 Projekte aus den Schwerpunktthemen „Detektion von Gefahrstoffen“ und „Schutzsysteme für Rettungskräfte“ angelaufen. Im Mittelpunkt des Forschungsthemas „Detektion von Gefahrstoffen“ steht die Entwicklung von Detektionssystemen für biologische, chemische oder explosive Substanzen. Ein wichtiger Entwicklungsansatz ist hierbei die Miniaturisierung. Sogenannte Lab-on-a-Chip-Systeme sollen Analysen, die gewöhnlich ein ganzes Labor erfordern, innerhalb kürzester Zeit und direkt vor Ort durchführen. Die Entwicklung von Detektionssystemen zum Aufspüren von gefährlichen Gegenständen und Gefahrstoffen auf Basis der Terahertz-Technologie bildet einen weiteren Forschungsschwerpunkt. Dabei werden





in einem Querschnittsprojekt[7] ethische Fragestellungen begleitend untersucht. So kann von Beginn an Einfluss auf die Entwicklung technologischer Lösungen genommen und deren erfolgreiche Umsetzung unterstützt werden.

Die Entwicklung innovativer Sicherheitslösungen, die die Leistungsfähigkeit und den Schutz von Einsatzkräften verbessern sollen, steht im Mittelpunkt des Schwerpunktthemas „Schutzsysteme für Sicherheits- und Rettungskräfte". Ein Förderschwerpunkt bildet hierbei die Integration von mobilen Ortungssystemen und Sensoren zur Messung der Vitalfunktionen in die Schutzbekleidung. Zusätzlich muss die Kleidung wie etwa im Falle von Feuerwehrmännern Schutz vor Hitze bieten und darf die Feuerwehrleute nicht bei ihrer Arbeit behindern. Um diese Vielzahl von Materialanforderungen erfüllen zu können, bedarf es der Entwicklung neuer, speziell auf die Einsatzbedingungen zugeschnittener Hochleistungstextilien, die ihre Einsatzfähigkeit und Robustheit in umfangreichen Praxistests unter Beweis stellen müssen.

Abbildung 2: Projektbeispiele



Projektbeispiel aus dem Schwerpunkt „Schutz von Verkehrsinfrastrukturen": OrGaMIR

Bei der Gefahrenabwehr in der U-Bahn gilt der eingeschränkte Zugang zum Einsatzort als größtes Hindernis für Rettungsoperationen. Die Rettungskräfte benötigen exakte und zuverlässige Informationen über die Nutzbarkeit bzw. eventuelle Kontaminationen von Rettungswegen. In dem Projekt „OrGaMIR" wird unter der Leitung der Universität Paderborn gemeinsam mit Partnern aus Wissenschaft und Wirtschaft, U-Bahn-Betreibern und Feuerwehr ein innovativer Ansatz entwickelt, mit dem solche Informationen künftig früher zur Verfügung gestellt werden können. So werden schnellere und sicherere Evakuierungen ermöglicht. Im Notfall leitet das sogenannte OrGaMIR-System während der Selbstrettungsphase die Fahrgäste zu sicheren, nicht kontaminierten Ausgängen, zum Beispiel durch Durchsagen und optische Signale. Zur Umsetzung des Vorhabens gehören tunnelklimatische Untersuchungen, deren Ergebnisse in die Optimierung bestehender U-Bahnhof-Architekturen und die Verbesserung der Sicherheit neuer U-Bahnhöfe bei der Planungs- und Entwurfsphase eingehen. Link zur Projektseite: www.orgamir.de; Bildquelle: Universität Paderborn, C.I.K.

[7] Siehe auch http://www.izew.uni-tuebingen.de/kultur/theben.html.



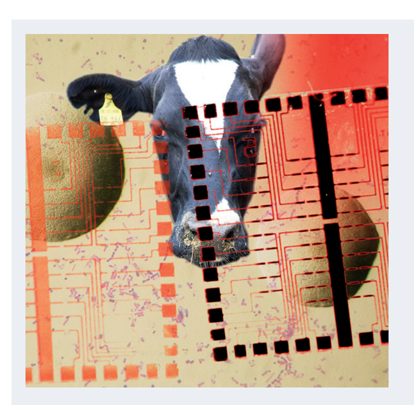




Projektbeispiel aus dem Schwerpunkt „Schutz und Rettung von Menschen“: Hermes

Einige Multifunktionsarenen verfügen über Zuschauerkapazitäten von weit über 50.000 Zuschauern. Im Notfall kann es bei der Evakuierung der Menschen bei Überbelegung oder Ausfall einzelner Rettungswege zu gefährlich hohen Personendichten und lang anhaltenden Stauungen kommen. Im Projekt „HERMES“ soll unter der Leitung des Jülich Supercomputing Centre (JSC) am Beispiel der Multifunktionsarena in Düsseldorf gezeigt werden, wie bei Großveranstaltungen Menschenmassen gezielt geführt werden können, sodass eine bestmögliche Ausnutzung der Rettungswege erreicht werden kann. Ziel des Verbundprojektes ist es, mit Partnern aus Wissenschaft und Wirtschaft einen Evakuierungsassistenten zu entwickeln, der Entscheidungsträger (Betreiber, Sicherheitsdienste, Polizei und Feuerwehr) durch frühzeitige Stauprognosen dabei unterstützt, die Lage richtig einzuschätzen und die Rettungskräfte optimal einzusetzen. Zusätzlich soll die Möglichkeit gegeben sein, schon im Vorfeld der Veranstaltungen mögliche Gefahrensituationen analysieren zu können. Link zur Projektseite: www.fz-juelich.de/jsc/appliedmath/ped/projects/hermes; Bildquelle: LTU arena



Projektbeispiel aus dem Schwerpunkt „Detektion von Gefahrstoffen“: ATLAS

Die Landwirtschaft zählt, besonders im Hinblick auf biologische Gefährdungen, zu den kritischen, für die Versorgung der Bevölkerung relevanten Infrastrukturen. Im Fall von Tierseuchen können die wirtschaftlichen Folgen, genauso wie die Verunsicherung der Bevölkerung, erheblich sein. Aus diesem Grund soll im Projekt „ATLAS“ unter der Leitung des Friedrich-Loeffler-Instituts gemeinsam mit Partnern aus Wissenschaft und Wirtschaft ein neuartiges Detektionssystem entwickelt werden, das den Nachweis verschiedener Tierseuchen vor Ort erlaubt. Durch die Miniaturisierung eines Labors in Form eines Chips (Lab-on-a-Chip-System) soll eine schnelle und flexible Reaktion auf mögliche biologische Bedrohungslagen durch Tierseuchenerreger oder chemische Gefahrenstoffe erreicht werden. Link zur Projektseite: www.fli.bund.de; Bildquelle: Foto Jan-Peter Kasper, dpa; Fotomontage Wolfram Maginot, FLI





Disziplinen aus den Geistes- und Sozialwissenschaften, den Verhaltens- und Kulturwissenschaften sowie den Wirtschafts- und Rechtswissenschaften befassen sich mit gesellschaftswissenschaftlichen Themen der Sicherheitsforschung. Nach einer Analyse wurden diese Themen den vier Säulen „Sicherheitskultur", „Architektur", „Organisation" und „Technik" zugeordnet (vgl. Abbildung 3). Insbesondere Fragestellungen der Säulen „Organisation" und „Technik" sowie Fragen zur Akzeptanz der Technologieentwicklungen, zu Quellen von Bedrohungen, zum Datenschutz oder zur Auswirkung auf die Menschen- und Freiheitsrechte werden entweder in den Projekten integriert oder als Querschnittsprojekt begleitend zu mehreren Verbundprojekten untersucht.

Die Forschungsthemen in den Säulen „Sicherheitskultur" und „institutionelle Sicherheitsarchitektur" wurden in einer eigenen Förderbekanntmachung ausgeschrieben.

Abbildung 3: Vier-Säulen-Modell der gesellschaftlichen Dimensionen der Sicherheitsforschung




Theoriebezug
Reflexion auf alle vier Dimensionen unter
gegenwartsdiagnostischen, kulturalistischen, system-, macht-, wissens- und medientheoretischen Aspekten

Sicherheitskultur (gesellschaftliche Ebene)	Architektur (international, national)	Organisation (operativ)	Technik (Mikroebene)
Gesellschaftspolitische Ebene – soziale und politische Konflikte – Sicherheitsökonomie Bedrohungswahrnehmung/ Sicherheitskommunikation – gesellschaftliche Sicherheitserwartungen – objektive vs. subjektive Sicherheit Definitionen konkreter Bedrohungs-/Gefährdungslagen, Krisenherde – Terrorismus, organisierte Kriminalität, illegale Migration – Natur und Technik Ursachenbestimmung von Gewalt/Kriminalität Aspekte von Sicherheitstechnologien – Akzeptanz: ökonomisch, sozial, politisch, kulturell – Folgen: ökonomisch, sozial, politisch, kulturell; Evaluation Funktionalität	Staatliche Ebene – Gewaltmonopol – Ressourcen (Demographie, Finanzen) Institutionelle Ebene – Hoheitlich-privat-NGO – Spezifische Architekturen (z.B. Katastrophenschutz usw.) Räumliche Ebene – Stadt/öffentlicher Raum – Geopolitische Dimension (Konflikte)	Institutionelle Rahmen – Verwaltung, Organisation, Recht – Organisatorisches Prozedieren (organisationsintern/-extern) Kommunikation/Handeln/ Wissen – Sozio-technische Bedingungen (Medien, Technik) – Organisationsspezifische Prozedere Kulturen – Unternehmens-, Organisationskulturen – Sicherheits-/Risikokulturen Ressourcen – Personal/Teambildung – Ökonomie	Technikgenese – Leitbilder – Normierung/Standardisierung – Leistungserwartungen Technikakzeptanz – politisch-juridische Akzeptanz – ökonomische Aspekte der Akzeptanz – sozial-kulturelle Aspekte der Akzeptanz Technikimplementierung – Soziotechnische Integration: Kommunikationsaspekt – Soziotechnische Integration: Kooperationsaspekt – Soziotechnische Integration: Kompetenzen Technikfolgen – ökonomische Folgen – soziale und kulturelle Folgen – politische Folgen

Quer zu den einzelnen Säulen liegende programmatische Aspekte der Forschung im Rahmen des BMBF-Programms.





Weitere Schwerpunktthemen, zum Beispiel zum Schutz von Versorgungsinfrastrukturen, zur Mustererkennung oder zum Schutz von Warenketten, wurden ausgeschrieben. Der aktuelle Stand der Projektförderung ist in Abbildung 4 zusammengefasst.

Abbildung 4: Aktueller Stand der Projektförderung in der Sicherheitsforschung (Stand: Ende Juni 2009)

SZENARIOORIENTIERTE FÖRDERUNG	TECHNOLOGIEVERBÜNDE
Schutz von Verkehrsinfrastrukturen 10 Projekte mit 76 Einzelvorhaben in der Förderung Innovationsplattform gestartet	**Detektion von Gefahrstoffen** 19 Projekte mit 95 Einzelvorhaben in der Förderung
Schutz und Rettung von Menschen 14 Projekte mit 78 Einzelvorhaben in der Förderung Innovationsplattform gestartet	**Schutzsysteme für Sicherheits- und Rettungskräfte** 6 Projekte mit 52 Einzelvorhaben in der Förderung
Schutz vor Ausfall von Versorgungsinfrastrukturen Im März 2008 ausgeschrieben	**Mustererkennung** Im Mai 2008 ausgeschrieben
Sicherung der Warenketten Im Dezember 2008 ausgeschrieben	
Gesellschaftliche Dimensionen der Sicherheitsforschung Im Oktober 2008 ausgeschrieben	
Israelisch-Deutsche Forschungskooperation Im Dezember 2008 ausgeschrieben	

1.3.2 INTERNATIONALE KOOPERATIONEN

Deutschland strebt auf dem Gebiet der zivilen Sicherheitsforschung eine aktive Rolle bei der Entwicklung von Lösungsansätzen für globale Herausforderungen wie den internationalen Terrorismus an, auch durch internationale Kooperationen.[8] In der Forschungszusammenarbeit im Rahmen bilateraler Kooperationen gilt es, gemeinsame Stärken zu nutzen, um Forschung und Innovation zu gestalten und gleichzeitig sicherzustellen, dass Sicherheitslösungen nicht an den Bedürfnissen der internationalen Märkte vorbei entwickelt werden. Die bilaterale Kooperation wird in einem ersten Schritt insbesondere mit Staaten aufgebaut, die spezifische Stärken in der zivilen Sicherheitsforschung aufweisen.

So hat die Bundesregierung am 16. März 2009 ein Regierungsabkommen mit der neuen US-Regierung zur transatlantischen Kooperation in der Sicherheitsforschung unterzeichnet, in dem eine enge wissenschaftliche und technologische Zusammenarbeit vereinbart wurde. Die entsprechenden Arbeitsprogramme werden derzeit bearbeitet.




8 Vgl. http://www.bmbf.de/de/13409.php.







Als weiterer strategischer Schwerpunkt bei der Anbahnung internationaler Forschungsallianzen wird die Kooperation zwischen Deutschland und Israel im Bereich der zivilen Sicherheit ausgebaut. Eine erste Bekanntmachung[9] zu diesem Thema wurde bereits im Dezember 2008 veröffentlicht. Vorrangiges Ziel der von beiden Staaten getragenen Förderung ist die Entwicklung innovativer Lösungen zum Schutz der zivilen Bevölkerung und kritischer Infrastrukturen sowie für den Einsatz im Katastrophenschutz und Krisenmanagement. Eine erste offizielle Zusammenarbeit zwischen deutschen und israelischen Forschungsgruppen ist bereits mit dem Start des Projektes „ChipSenSiTek" angestoßen worden. Ziel dieses Pilotprojektes – angesiedelt im Förderschwerpunkt „Detektion von Gefahrstoffen"[10] – ist die Entwicklung eines chip-basierten Gassensorensystems zur Detektion von Explosiv- und Sprengstoffen, das bei Zugangskontrollen auf Flughäfen oder in anderen Gebäuden eingesetzt werden soll.

Auch auf europäischer Ebene wird der Ausbau bilateraler Forschungskooperationen forciert. Um Synergien in der zivilen Sicherheitsforschung besser nutzen zu können, strebt das Bundesministerium für Bildung und Forschung hier insbesondere enge Partnerschaften mit denjenigen europäischen Staaten an, die ebenfalls über eigenständige nationale Forschungsprogramme im Bereich der zivilen Sicherheit verfügen. So ist im Januar 2009 seitens des Bundesministeriums für Bildung und Forschung und der Agence nationale française de la recherche (ANR) eine Kooperationsvereinbarung zwischen Deutschland und Frankreich unterzeichnet worden. Ziel ist die wechselseitige Öffnung der Sicherheitsforschungsprogramme sowohl in Deutschland als auch in Frankreich. Im Rahmen der Bekanntmachung des Bundesministeriums für Bildung und Forschung „Sicherung der Warenketten" und des ANR Calls „CSOSG 2009 – Theme Axis: Securing the Logistics Chain" hatten französische und deutsche Forschergruppen erstmalig die Möglichkeit, gemeinsame Anträge zu stellen.



1.3.3 GESELLSCHAFTLICHER DIALOG

Der Dialog zwischen den Beteiligten war von Beginn an, bereits bei der Erstellung des Programms, ein entscheidendes Element. In einem Agendaprozess identifizierten über 250 Fachleute disziplinübergreifend in einem offenen Verfahren die vorrangigen Forschungsthemen in der zivilen Sicherheit. In der Umsetzung des Programms spiegelt sich der Dialogprozess zu den gesellschaftlichen Fragen der Sicherheitsforschung auf verschiedenen Ebenen wider:

Auf der Ebene der Forschungsprojekte ist der Dialog zwischen den verschiedenen Akteuren ein projektimmanenter Bestandteil: sowohl horizontal durch die Erarbeitung gemeinsamer Lösungsansätze der Ingenieur- und Naturwissenschaften im Dialog mit

 Vgl. http://www.bmbf.de/foerderungen/13281.php.

 Vgl. http://www.bmbf.de/de/12917.php.





Geistes- und Sozialwissenschaften als auch vertikal durch die Einleitung einer gemeinsamen Diskussion aller Akteure aus Forschung, Wirtschaft und Endnutzerkreis zu den gesellschaftlichen Auswirkungen innovativer Sicherheitslösungen und -technologien. Der Dialog zwischen den Projekten und weiteren Akteuren, die nicht direkt in die Projekte involviert sind, wird durch sogenannte Innovationsplattformen unterstützt.

Im Rahmen des gesellschaftlichen Dialogs werden immer wieder grundlegende gesellschaftliche Fragen in der Sicherheitsforschung betrachtet und öffentlichkeitswirksam diskutiert. So hat das Bundesministerium für Bildung und Forschung im November 2008 mit dem Kongress „... mit Sicherheit: für Freiheit – Die gesellschaftlichen Dimensionen der Sicherheitsforschung“ die Debatte um Grundsatzfragen wie zu Entwicklungen der gesellschaftlichen Sicherheitskultur und der institutionellen Sicherheitsarchitektur eröffnet. Da gerade der Forschung zu gesellschaftlichen Fragestellungen ein hoher Stellenwert beigemessen wird, sind solche Austauschmöglichkeiten auch in Zukunft entscheidend. Sie sind Anstoß für Gespräche und bieten die Chance, mehr über Wünsche, Erwartungen und auch Schwierigkeiten im Hinblick auf die Forschung für die zivile Sicherheit von Akteuren wie Bürgern zu erfahren.

Der öffentliche Dialog informiert so transparent wie möglich über die Themen der Sicherheitsforschung. Er soll dazu beitragen, in der Öffentlichkeit ein besseres Verständnis für die Herausforderungen und Chancen eines – auch durch Hightech – verbesserten Schutzes der Zivilgesellschaft zu erzeugen, und gleichzeitig das Spannungsfeld zwischen Sicherheit und Freiheit im Blick haben.

Ein wichtiger Baustein im Dialog und in der Vermittlung gesellschaftlich relevanter Forschungsthemen bildet der Internetauftritt des Bundesministeriums für Bildung und Forschung zur Sicherheitsforschung – www.sicherheitsforschungsprogramm.de.[11] Ziel des Internetangebotes ist insbesondere das lückenlose Bereitstellen von Informationen zu allen Aktivitäten und Fördermaßnahmen innerhalb des Sicherheitsforschungsprogramms.

Begleitend zu den online verfügbaren Hintergrundinformationen werden in einer neuen Publikationsreihe die einzelnen Projekte der verschiedenen Förderschwerpunkte des Programms in vertiefter Form vorgestellt. Erschienen sind bisher vier – über das Internet zu beziehende – Ausgaben zu den Förderschwerpunkten „Detektion von Gefahrstoffen“, „Schutz von Verkehrsinfrastrukturen“, „Schutzsysteme für Sicherheits- und Rettungskräfte“ und „Schutz und Rettung von Menschen“. Zusätzlich werden alle in der zivilen Sicherheitsforschung vertretenen Akteure und interessierten Bürger über den regelmäßig erscheinenden „Informationsbrief zur Sicherheitsforschung“ über alle wichtigen Neuigkeiten rund um das nationale und das europäische Sicherheitsforschungsprogramm informiert.

[11] Vgl. darüber hinaus http://www.bmbf.de/de/6293.php.









1.3.4 INNOVATIONSPLATTFORMEN

Um die erfolgreiche Umsetzung von Forschungsergebnissen in praxistaugliche und vermarktbare Produkte und Verfahren zu unterstützen, werden zu den szenarienorientierten Schwerpunktthemen Innovationsplattformen eingerichtet. Bereits im September 2008 startete die Innovationsplattform „Schutz von Verkehrsinfrastrukturen", im Juni 2009 folgte der Auftakt zur Innovationsplattform „Schutz und Rettung von Menschen".

Als neues Instrument im Rahmen der Hightech-Strategie der Bundesregierung dienen die Innovationsplattformen dazu, den Aufbau strategischer Partnerschaften zwischen Endnutzern, Industrie und Wissenschaft zu fördern. Keimzelle einer jeden Innovationsplattform sind die Verbundprojekte der szenarioorientierten Schwerpunkte des zivilen Sicherheitsforschungsprogramms. Unter dem Leitmotiv „Von der Forschung aus vorausdenken" bieten die Innovationsplattformen allen interessierten Akteuren aus Forschung, Industrie, den Behörden und Organisationen mit Sicherheitsaufgaben und weiteren zuständigen Bundes- und Landesressorts bzw. deren nachgeordneten Bereichen die Möglichkeit, innovative Sicherheitslösungen bereits in der Frühphase der Entwicklung mitzugestalten.





Dabei können Rahmenbedingungen der künftigen Umsetzung, die Anforderungen des künftigen Marktes und die künftige gesellschaftliche Einbettung neuer, in der Forschung entstehender Lösungen diskutiert und so Impulse für die erfolgreiche Umsetzung von Forschungsergebnissen gesetzt werden. Zudem bietet das Forum allen Akteuren die Möglichkeit, die künftige Ausrichtung der Forschung im jeweiligen Themenfeld mitzugestalten.

Die Innovationsplattformen dienen der Vernetzung und dem Informationsaustausch zwischen den geförderten Verbundprojekten. So sollen Synergien zwischen themenverwandten Forschungsprojekten erschlossen und Kooperationen, die über die geförderten Projekte hinausgehen, angeregt werden. Sie tragen zudem zur Bildung einer nationalen Fachszene in diesem verhältnismäßig jungen Forschungsfeld bei. Die Innovationsplattformen gründen zu spezifischen Fragestellungen Arbeitsgruppen, die Strategiepapiere, Roadmaps und Handlungsoptionen erarbeiten.

Die im September 2008 gestartete Innovationsplattform „Schutz von Verkehrsinfrastrukturen" zählt mittlerweile rund 240 Mitglieder. 33 Prozent der Akteure repräsentieren öffentliche oder private Endnutzer, 42 Prozent der Akteure kommen aus der Forschung, 25 Prozent aus der Industrie. Bereits während der Auftaktveranstaltung konstituierten sich analog zu den vier geförderten Verkehrsträgern die Arbeitsgruppen „Luftverkehr", „Schienenverkehr", „Seeverkehr" und „Straßenverkehr". Ein Schwerpunkt ihrer thematischen Arbeit war die Bestandsaufnahme der deutschen und internationalen Forschungslandschaft sowie die Identifikation zukünftiger Forschungsbedarfe. Zu den identifizierten Fragestellungen zählen technologisch geprägte Themen wie Detektion, Videoüberwachung, Datenfusion und Gebäudesensorik. Dazu kommen aber auch





gesellschaftswissenschaftlich orientierte Bereiche wie Personenstromlenkung, Haltestellendesign und Haftungsrecht sowie übergreifende Themen wie integrierte Sicherheitsmanagementkonzepte oder Modellierung und Simulation. Anhand der erarbeiteten Ergebnisse werden die Arbeitsgruppen eine SWOT-Analyse durchführen und Handlungsempfehlungen ableiten, die die Weiterentwicklung der nationalen und europäischen Sicherheitsforschung zum Schutz von Verkehrsinfrastrukturen unterstützen werden.

Um den Transfer der Forschungsergebnisse in die Anwendung zu unterstützen, hat die Innovationsplattform „Schutz von Verkehrsinfrastrukturen“ in einem ersten Schritt die Chancen einer frühzeitigen, entwicklungsbegleitenden Normung und Standardisierung diskutiert und eine Kooperation der geförderten Verbundprojekte mit dem Deutschen Institut für Normung e. V. (DIN) entschieden.

1.4 AUSBLICK

Das Programm der Bundesregierung „Forschung für die zivile Sicherheit“ ist mit dem Start erster Förderprojekte und Innovationsplattformen erfolgreich angelaufen und wird bis Ende der ersten Förderphase wichtige Meilensteine in der zivilen Sicherheitsforschung in Deutschland setzen. Bereits jetzt zeigt die positive Resonanz der an den Projekten beteiligten Forschungsakteure, dass insbesondere die anwendungs- und endnutzerorientierte Ausrichtung des Programms sowie die gezielte Verknüpfung technologischer und gesellschaftlicher Fragestellungen in den Forschungsprojekten sich nachhaltig bewährt haben. Ebenfalls bewährt hat sich die seit dem Agendaprozess 2006 konsequent verfolgte Einbindung aller in der zivilen Sicherheit relevanten Akteure und gesellschaftlichen Gruppen – nicht zuletzt durch den seitens des Bundesministeriums für Bildung und Forschung eingeleiteten Dialogprozess zu den gesellschaftlichen Fragen der Sicherheitsforschung. An diesem Modell will das Bundesministerium für Bildung und Forschung auch in der kommenden zweiten Förderperiode festhalten und für die Fortschreibung des Programms frühzeitig alle Forschungsakteure, Endnutzer und zuständigen Ressorts einbinden.



1.5 LITERATUR

BMBF 2007a
Bundesministerium für Bildung und Forschung (BMBF) Referat Öffentlichkeitsarbeit (Hrsg.): Forschungsunion Wirtschaft – Wissenschaft, Bonn, Berlin 2007. URL: http://www.bmbf.de/pub/forschungsunion_wirtschaft_wissenschaft.pdf [Stand: 22.07.2009].

BMBF 2007b
Bundesministerium für Bildung und Forschung (BMBF) Referat Öffentlichkeitsarbeit (Hrsg.): Die Hightech-Strategie für Deutschland – Erster Fortschrittbericht, (Broschüre), Bonn, Berlin, 2007.





BMBF 2007c
Bundesministerium für Bildung und Forschung (BMBF) Referat Öffentlichkeitsarbeit (Hrsg.): Forschung für zivile Sicherheit. Programm der Bundesregierung, (Programmbroschüre), Bonn, Berlin, 2007.

BMBF 2007d
Bundesministerium für Bildung und Forschung (BMBF) Referat Öffentlichkeitsarbeit (Hrsg.): Forschung für zivile Sicherheit. Eine Bestandsaufnahme: Forschungslandschaft und Ansprechpartner, (Broschüre), Bonn, Berlin, 2007.

BMBF 2008a
Bundesministerium für Bildung und Forschung (BMBF) Referat Sicherheitsforschung (Hrsg.): Forschung für zivile Sicherheit. Detektion von Gefahrstoffen, (Projektbroschüre), Bonn, Berlin, 2008.

BMBF 2008b
Bundesministerium für Bildung und Forschung (BMBF) Referat Sicherheitsforschung (Hrsg.): Forschung für zivile Sicherheit. Schutz von Verkehrsinfrastrukturen, (Projektbroschüre), Bonn, Berlin, 2008.



BMBF 2009a
Bundesministerium für Bildung und Forschung (BMBF) Referat Sicherheitsforschung (Hrsg.): Forschung für zivile Sicherheit, Schutzsysteme für Sicherheits- und Rettungskräfte, (Projektbroschüre), Bonn,Berlin, 2009.

BMBF 2009b
Bundesministerium für Bildung und Forschung (BMBF): Abkommen zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Vereinigten Staaten von Amerika über die wissenschaftliche und technologische Zusammenarbeit auf dem Gebiet der zivilen Sicherheit, Bonn, 2009. URL: http://www.bmbf.de/pub/BGBL_II_11_05_09.pdf [Stand: 22.7.2009].

Forschungsunion Wirtschaft – Wissenschaft 2009
Forschungsunion Wirtschaft – Wissenschaft (Hrsg.): Woher das neue Wachstum kommt. Innovationspolitische Impulse für ein starkes Deutschland in der Welt, (Broschüre), Berlin, 2009.





2 HERAUSFORDERUNGEN FÜR DIE ZIVILE SICHERHEITS-WIRTSCHAFT UND -WISSENSCHAFT IN DEUTSCHLAND

STEFAN VON SENGER UND ETTERLIN

2.1 SICHERHEIT ALS BREITES, ABER NICHT ALLUMFASSENDES FELD VERSTEHEN

Mit der Sicherheitsindustrie und Sicherheitswissenschaft beginnt sich eine neue Querschnittsbranche zu bilden, deren genaue Eingrenzung genauso schwierig ist wie die sinnvolle Verknüpfung ihrer unterschiedlichen Elemente zu ökonomisch und organisatorisch effizienten Einheiten. Was gehört alles dazu und was nicht? Definitionen von Sicherheit gibt es viele; in den meisten Fällen kann man sich auf einen Kernbestandteil einigen: Es geht um Bekämpfung von Kriminalität, Organisierter Kriminalität und Terrorismus, um den Schutz vor Naturkatastrophen, Pandemien und Industrieunfällen, um Brandschutz, IT-Sicherheit und Schutz von kritischen Infrastrukturen. Was ebenfalls allgemein angenommen wird, ist, dass es eine feste Grenzziehung der zivilen Sicherheit zur militärischen gibt – zu Unrecht, wie wir sehen werden. Ausgenommen von der Diskussion werden meistens die großen Felder Gesundheit und Verkehr, obwohl es auch hier um Prävention, Schutz und Wiederherstellung von „Normal"-Zuständen geht.

Sind die klassischen Felder der Inneren Sicherheit – erweitert durch solche der Betriebssicherheit zivilisatorischer Systeme – schon für sich genommen breit genug, wird es erst richtig spannend an den bisherigen Rändern dieses Kernbestands von Sicherheit: Da spielt zum Beispiel der Einsatz von Kapazitäten und Fähigkeiten des Militärs eine nicht ganz unwichtige Rolle. Der Abschuss eines durch Terroristen gekaperten Flugzeugs ist in Deutschland zwar verfassungsrechtlich verboten worden, aber möglich gewesen wäre er nur durch die Bundeswehr. Drohende und eingetretene Schäden durch Überschwemmungen an Oder, Elbe oder Rhein, durch Sturmfluten an der Küste oder Orkane in den Mittelgebirgen können meist nur durch den Einsatz der Bundeswehr bekämpft oder behoben werden. Der denkbare Einsatz von chemischen und biologischen Schadstoffen durch Terroristen gegen die Zivilbevölkerung könnte ebenfalls nur durch die ABC-Truppen der Verteidiger bekämpft werden. Es gibt also eine Menge denkbarer Bedrohungsszenarien, in denen zivile Sicherheit nur mit militärischen Mitteln erreicht werden kann. Umgekehrt erfahren die Soldaten von ISAF, UNIFIL, KFOR und anderen Auslandsmissionen, dass ihre Aufgaben in asymmetrischen Auseinandersetzungen oftmals in die Nähe von Polizeiaufgaben kommen und dass sie mit vielen anderen Sicherheits-



kräften und Hilfsorganisationen eine „vernetzte Sicherheit" schaffen müssen. Die Grenze zwischen innerer und äußerer Sicherheit war schon immer fließend; sie verschwimmt heutzutage zunehmend.

Ein weiteres Gebiet, das ganz offensichtlich unsere zivile Sicherheit bedroht, das aber normalerweise nicht in die Sicherheitsdiskussion mit einbezogen wird, ist der Klimawandel. Dabei scheint der Klimawandel mannigfache neue Bedrohungen mit sich zu bringen, vermehrte Unwetter, eine sich wandelnde Pflanzen- und Tierwelt auch in unseren Breitengraden mit neuen Krankheitserregern und Schädlingen, für die unsere Biozönosen nicht gewappnet sind. Selbstverständlich ist solchen Gefahren mit den klassischen Mitteln der Sicherheitstechnik nicht beizukommen. Maßnahmen zur Senkung der Emission von Treibhausgasen gehören, so scheint es, nun wirklich nicht mehr in den Horizont der zivilen Sicherheitstechnik. Und dennoch: Überschneidungen gibt es auch hier. Die präventive Beschaffung von und Ausbildung an Geräten zur Abstandserkennung von erhöhten Körpertemperaturen hat zum Beispiel dazu geführt, dass der Inselstaat Singapur vor einigen Jahren weitgehend von den Schrecknissen der damals grassierenden asiatischen Vogelgrippe verschont geblieben ist, während andere, ärmere und weniger gut organisierte Länder diese Vorsichtsmaßnahmen nicht ergriffen und viele Opfer zu beklagen hatten. Jeder Fluggast, der nach Singapur gelangte, musste nämlich solche, für den Organismus völlig unschädliche Geräte passieren, und wer erhöhte Temperatur hatte, wurde herausgegriffen, untersucht sowie nötigenfalls in Quarantäne gesteckt und behandelt. Deutschland hatte derartige Geräte auch nicht; an Flughäfen oder an den Landungsbrücken von Überseehäfen hätten sie aber durchaus Sinn haben können.




Die Ansteckungsgefahr bei Vogelgrippe und anderen Krankheitserregern hängt nicht in erster Linie vom Klimawandel ab, sofern sich nicht Vogelfluglinien verändern sollten. Vielmehr ist sie Folge der Globalisierung aller Lebensbereiche, insbesondere des stetig steigenden Welthandels und internationalen Reiseverkehrs. Ein nicht unbeträchtlicher Teil davon wird über den Luftweg abgewickelt, so dass die Emissionen von CO2 und Stickoxid in der besonders empfindlichen unteren Stratosphäre ständig steigen. Erhöhte Mobilität bringt somit neue Freiheiten, aber auch neue Gefahren und Abhängigkeiten, die sich zu Sicherheitsbedrohungen auswachsen können, sei es als Klimawandel, als Verbreitung von Schädlingen und Krankheiten oder als Bedrohung der über Pipelines oder Tankerschiffe abgewickelten Versorgung mit den Energieträgern Erdöl und Erdgas.

In der Sicherheit scheint alles mit allem zusammenzuhängen; die zivile Sicherheit ist mit der militärischen verwoben, unsere globalisierte Lebens- und Wirtschaftsweise leistet dem Klimawandel Vorschub und schafft dadurch neue Sicherheitsrisiken. Insofern kann man auch die Themen Verkehr und Gesundheit nicht ganz außen vor lassen, denn Technologien zu größerer Verkehrseffizienz können zum Beispiel Emissionen vermeiden und dadurch die Auswirkungen des Klimawandels begrenzen helfen. Darüber hinaus





trägt die Kontrolle von Holzverpackungen und -paletten im internationalen Seeverkehr auf Schädlinge dazu bei, Flora und Fauna zu schützen, um die Lebensmittelversorgung zu sichern.

Gleichwohl sollte man nicht alles mit allem vermischen und nicht „Sicherheit" als die große neue, alles umfassende Politikkategorie einführen. Das wäre schrecklich: nicht nur intellektuell fragwürdig, sondern auch demokratiegefährdend. Schon gibt es in Romanform eine negative Utopie einer solchen Entwicklung, ganz in der Tradition von George Orwells „1984" oder Aldous Huxleys „Schöne neue Welt". Das jüngst publizierte Buch „Corpus Delicti: Ein Prozess" von Juli Zeh beschreibt den totalen Präventionsstaat in der Mitte des 21. Jahrhunderts. Nach dem Ende aller Ideologien – Sozialismus, Kapitalismus usw. haben ausgedient – nimmt sich der Staat die Aufgabe des Schutzes vor allen möglichen Gefahren als zentralen Bindekitt, als eigentliche, letzte Legitimation. Da werden die Menschen ständig ermahnt und gewarnt, aber auch bestraft, wenn sie nicht jeden Tag ihren Blutdruck messen, ihre Virenupdates hochladen und nicht überall und zu jeder Zeit über GPS (bzw. dessen Nachfolgetechnik) auffindbar sind. Vorstufen zu all diesen Technologien kennen wir schon heute zu Genüge. Aber wollen kann ein solches lückenloses System der wohlwollenden Überwachung keiner von uns.





Die Schnittstellen von zivilen und militärischen Mitteln zur Sicherheit, von Maßnahmen zur Herstellung einer wie auch immer gearteten Rundumprävention gegen Kriminalität, Krankheit oder Unfälle haben auch inhärente Grenzen: Der Polizist wird zum Ort eines Verbrechens oder eines Unfalls gerufen, wenn das Ereignis passiert ist. Er hat dann vor Ort Hilfe zu leisten, auch auf Folgeerscheinungen des singulären Ereignisses zu achten. Der Ernstfall eines Soldaten sieht dagegen vollkommen anders aus: Kriegerische Auseinandersetzungen sind meist länger anhaltende Zustände, mit ständig wechselnden Gefahren für Leib und Leben, bei denen die Bedrohung gerade nicht aufhört, wenn ein Ereignis stattgefunden hat; das gilt selbst für den asymmetrischen Krieg. Ähnlich kann man Maßnahmen für den Klimaschutz oder für die Verkehrssicherheit (immerhin nehmen wir es weitgehend unbeteiligt hin, wenn es jedes Jahr auf unseren Straßen an die 5.000 Tote und zehntausende Schwerverletzte gibt) nicht so ohne Weiteres unter die Rubrik „zivile Sicherheit" subsumieren, weil Ursachen, Bekämpfungsmethoden und Technologien sich zu sehr von den klassischen Feldern der inneren Sicherheit unterscheiden. Beispiele für Überschneidungen gibt es immer, aber es stellt sich doch die Frage, was man gewinnt, wenn man alles mit allem in Beziehung setzt. Weder zielgruppengenaue Produktentwicklung, noch gewissenhafte politische Prioritätensetzung sind auf dieser Grundlage möglich.

Auch angesichts der von manchen geforderten Auflösung oder Verschmelzung der Begriffe „Security" und „Safety" sind Zweifel angebracht. Sicherlich gibt es zahlreiche Beispiele, in denen das eine in das andere übergeht, ja sich sogar gegenseitig bedingt. Ein Bombenattentat auf ein Gebäude – als ein Security-Thema – kann erst dann seine





volle Wirksamkeit entfalten, wenn die Architektur viel Glas, wenig Versteifungsfestigkeit im Stahlskelett oder mangelnden Brandschutz vorgesehen hat – was ein Safety-Thema wäre. Das Einknicken von Überland-Stromleitungen durch Schneelast oder Wind (Safety) kann zu Blackouts führen, die Alarmsysteme und Kommunikationsnetze außer Gefecht setzen und so ganze Stadtteile zumindest zeitweise zu offenen Räumen für Einbruchskriminalität machen (Security). Gleichwohl muss nicht jede Brandschutzregel Schutz vor terroristischen Angriffen mitbedenken und es muss nicht das Stromnetz nur deshalb redundant und selbstheilend ausgelegt werden, um Alarmanlagen in Villenvierteln gängig zu halten.

In Brandenburg ist die ZukunftsAgentur Brandenburg GmbH – die Wirtschaftsfördergesellschaft des Landes – dabei, in verschiedenen Branchennetzwerken, die sich mit Aspekten von Sicherheit befassen (Logistik, Geoinformation, IKT), Denkprozesse darüber anzustoßen, inwiefern es zwischen den neuen Technologien, die in den Branchen entwickelt und eingesetzt werden, und dem Sicherheitsthema Synergien gibt. Dabei ist festzustellen, dass „Security"-Technologien überhaupt erst dann wirklich akzeptiert werden – soweit sie nicht gesetzlich vorgeschrieben sind –, wenn sie zugleich wirtschaftlich positive Effekte auch auf andere Abläufe und Ergebnisse in den Unternehmen haben. Videoüberwachungsanlagen in großen Güterverkehrszentren können zum Beispiel auch zum Wiederauffinden bestimmter Paletten und Chargen genutzt werden, Brandschutzsensoren auch zur Temperaturüberwachung für hitzeempfindliche Waren. Das Interessante dabei ist, dass Sicherheitstechnologien in vielen Bereichen erst dann wirklich eine Chance haben, wenn sie aus dem Massenmarkt kommen, was heißt, dass sie kostengünstig, standardisiert, bedienungsfreundlich und schnell ersetzbar sein müssen. Diese Eigenschaften haben sie häufig dann, wenn sie aus dem Safety-Bereich kommen, denn hier führen zum Beispiel arbeitsschutzrechtliche oder verkehrstechnische Vorgaben zu massenhaften Anwendungen und damit zu industriell interessanten Skaleneffekten. Es wird daher eine Herausforderung an die deutsche Politik sein, Marktimpulse für Sicherheitstechnologien so zu setzen, dass sie entweder aus dem Konsumentenmarkt kommen oder für ihn verwendbar sind.





Die genaue Betrachtung der Interferenzen der verschiedenen Randgebiete zum Thema zivile Sicherheit, aber auch der Überschneidungen zwischen vorsätzlichen Störungen der Sicherheit (Security) und zufälligen Schadensfällen (Safety) sowie, schließlich, der „Dual-use"-Möglichkeit von Konsumprodukten für den Massenmarkt und den Spezialanwendungen im Sicherheitsbereich bietet deswegen lohnenswerte Felder der Sicherheitsforschung. Die vielfältigen Beziehungen, Überschneidungen und Abhängigkeiten all dessen, was Sicherheit ausmachen kann, besser verstehen und beherrschen zu lernen, ist insofern die erste der großen Herausforderungen für die Sicherheitswirtschaft und -wissenschaft in Deutschland und Europa. Allerdings darf diese Klärung nicht zum Selbstzweck erfolgen, sondern muss der Erzielung höherer Effizienz und Stabilität der Systeme dienen.





2.2 TECHNIK DEM MENSCHEN ANPASSEN

Auf die Frage hin, was die Großstadt-Polizei an Fähigkeiten denn nun wirklich brauche, entgegnete die mir gegenüber sitzende Beamtin des höheren Dienstes der Berliner Landespolizei mit wenigen, eindeutigen Worten: „Kollegen mit Migrationshintergrund!“. Das war einigermaßen verblüffend, denn wir sprachen über Forschungs- und Ausrüstungsbedarfe und die Erwartungen eines der wichtigen Endnutzer solcher neuen Gerätschaften. Aber der Befund war klar: Verbrechensbekämpfung ist eine Dienstleistung, „people´s business“, kein Produkt. Technik wird gebraucht, ja sie ist unabdingbar, denkt man an Waffen, Kommunikationsmittel, Lagezentren oder Forensik. Aber Technik ist nur ein Hilfsmittel; in der eigentlichen Arbeit der Polizei sind Spürsinn, Intelligenz, Menschenkenntnis, Führungskunst, Erfahrung, Taktik, Wissen und Mut im Grunde viel wichtigere Fähigkeiten. Kollegen zu gewinnen, die aus anderen Kulturräumen kommen, auch eher exotische Sprachen sprechen (zum Beispiel arabisch oder tschetschenisch), die aber trotzdem ausreichend in Deutschland sozialisiert sind, um sich nahtlos in die deutsche Polizeiarbeit einordnen zu können, ist in der Tat eine große Herausforderung. Wie anders kann man mit Kriminalität umgehen, wenn sie aus Einwanderergruppen kommt, wie kann man V-Männer in gewissen Milieus platzieren und wie die richtigen Präventionsstrategien entwickeln, wenn nicht zumindest mit Minimalkenntnissen aus deren Kulturen?




Ein anderes Erlebnis bestätigt die Erkenntnis, dass der Mensch immer noch wichtiger ist als die Technik: Jeder Fluggast, der sich am Tel Aviver Flughafen Ben Gurion einchecken will, wird zunächst von einer jungen Person in Zivil (meist sind es junge Frauen) begrüßt und angesprochen. In den wenigen Sekunden des ersten Eindrucks und in dem kurzen Gespräch, das folgt, entscheidet diese Person, welcher Risikokategorie man zugeordnet wird, und man erhält auf seinem Pass einen Aufkleber, auf dem eine Zahl von 1 – 5 steht. 5 ist nicht immer die höchste Risikostufe und 1 nicht immer die niedrigste; die Zahlen wechseln täglich oder stündlich ihre Bedeutung nach einem System, das nur den Sicherheitskräften bekannt ist. Je nach Einstufung wird man dann relativ einfach „durchgewunken“ oder nach allen Regeln der Kunst „auseinandergenommen“. Hier kommt dann die modernste und aufwendigste Technik zum Einsatz, die es weltweit gibt. Oberstes Ziel ist eine effiziente, das heißt ökonomische Identifizierung derjenigen Fluggäste, von denen Gefahr ausgehen könnte. Die teure Technik und die aufwendigen anderen Methoden, mit denen risikoeingestufte Personen durch den gesamten Flughafen hindurch beobachtet werden, sollen nicht unterschiedslos für alle Flughafennutzer eingesetzt werden. Das wäre vollkommen unökonomisch. Das entscheidende Moment dieser Methodik gleich zu Anfang ist hingegen die Beobachtung von Mensch zu Mensch, die emotionale Intelligenz, die dazugehört, und die psychologische Ausbildung im Lesen von Stressanzeichen. Jeder wird nun sagen, dass man sich täuschen kann, dass dies kein irrtumssicheres System ist und stark von der Tagesform der Sicherheitskräfte





abhängen mag oder von den Verstellungskünsten von Menschen, die Böses im Schilde führen. Aber zum System selbst gehört die Unsicherheit, die oftmals als Zufälligkeit oder Willkür erscheinende Einstufung in die Risikostufen. Und selbst bei niedriger Risikoeinstufung kann man das Pech haben, durch die Technik voll durchleuchtet zu werden. Zufall ist hier System.

Wenn auch die Technik dem Menschen angepasst sein muss, so bleibt doch unbenommen, dass neue Technologien immer wichtige Hilfsmittel sein werden, um Sicherheit zu wahren und wieder herzustellen oder ihre Bedrohungen zu bekämpfen. Dafür sind eine Reihe von Basistechnologien notwendig, zum Beispiel die Sensorik, die Robotik oder auch die Ionen-Mobilitäts-Spektroskopie. Mit ihrer Hilfe kann man unterschiedlichste Sicherheitsbedarfe technologisch lösen wie zum Beispiel die Beobachtung von Chemietanklagern durch fahrende Roboter oder die Detektion von chemisch-biologischen Kampfstoffen im Gepäck von Fluggästen. In all diesen Technologien hat Deutschland viel vorzuweisen. Die Ergebnisse der zweiten Ausschreibungsrunde im Sicherheitsprogramm des 7. Forschungsrahmenprogramms der EU zeigten, dass Projekte mit deutscher Beteiligung besonders erfolgreich bei Entwicklungsvorhaben für die „CBRNE"-Bekämpfung (chemische, biologische-radiologische, nukleare und explosive Gefahrstoffe) waren, ein Hinweis auf die wissenschaftliche und industrielle Stärke auf diesem Gebiet.[1] Solche Entwicklungen können aber auch für ganz andere Einsatzgebiete verwendet werden. Biochips auf Basis von Nanoröhrchen könnten zum Beispiel in der Lebensmitteltechnologie und damit in der Gesundheitsvorsorge eine wichtige Rolle spielen. Die Bilderkennungssysteme, die in mobilen Kleinrobotern oder fliegenden Drohnen Videobilder interpretieren und per Funk an Lagezentren weitergeben, könnten in der Verkehrsüberwachung oder bei Großveranstaltungen eingesetzt werden. Spin-offs aus der militärischen Forschung in zivile Anwendungen sind seit Jahrzehnten etwas ganz Normales. Doch auch die Basistechnologien der Sicherheitswirtschaft können von vornherein multidimensional gedacht und deshalb potenziell in sehr vielen Szenarien und in sehr vielen Industrien verwendet werden. Forschritte zum Beispiel in der Terahertz-Technologie, mit der man hofft, eines Tages Menschen scannen zu können, ohne sie, wie bei der Durchleuchtung mittels Röntgenstrahlen, zu schädigen, wären relevant für Sicherheitszwecke, könnten aber auch in der Medizintechnik und in der Materialtechnik eingesetzt werden.



Auch wenn Teilbereiche der Erforschung solcher Technologien durchaus noch Grundlagenforschung sind, haben wir es in der Regel mit angewandter Grundlagenforschung oder Anwendungsforschung zu tun. Der szenarienorientierte Ansatz des nationalen Sicherheitsforschungsprogramms ist deshalb richtig. Es wird von den wahrscheinlichsten

[1] VDI 2009.







Bedrohungsszenarien oder den realen Bedarfen der Sicherheitsnachfrager ausgegangen und die Wissenschaft ist aufgefordert, im Verbund mit Produzenten und Nachfragern Systeme zu entwickeln, die alsbald eine wirtschaftliche Anwendung finden können.

Dennoch bleibt wahr: Einfach nur mehr Technik schafft nicht unbedingt mehr Sicherheit. Die Broschüre des Bundesministeriums für Bildung und Forschung (BMBF) über das nationale Sicherheitsforschungsprogramm zählt selbst einige faszinierende Beispiele dafür auf:[2] Wer stärkere Bremsen im Auto hat, fährt deshalb gerne auch schneller und näher an den Vordermann auf, so dass am Ende kein Mehr an Sicherheit herauskommt. Die Evakuierung von Stadien kann über bessere Leitsysteme oder bestimmte Ortungsakustik verbessert werden, aber einer der Engpässe für ein schnelleres Verlassen der Ausgänge ist die menschliche Eigenschaft, erst einmal kurz inne zu halten, Luft zu holen und sich neu zu orientieren, nachdem man den Ausgang durchschritten hat. Erst dadurch entsteht ein Rückstau, weil man die Nachrückenden aufhält. Eine Lösung könnte darin bestehen, eine Säule vor dem Ausgang zu platzieren, weil das Publikum dann erst einmal auch daran vorbei will und man so für alle mehr Raum gewonnen hat.

Ähnlich verhält es sich mit dem „Feuerwehrmann der Zukunft". Noch hitzebeständigere Kleidung bei zugleich größerer Atmungsaktivität der Textilien, funkgesteuerte physiologische Überwachung und Ortung der Einsatzkräfte auch im dicksten Schlamassel können sinnvolle technologische Ergänzungen sein, um Menschenleben zu retten. Der „Hightech"-Feuerwehrmann droht aber auch am Ballast und an den Bedienungsanforderungen seiner Ausrüstung zu ersticken. Zum Teil sehen wir diese Folgen heute schon beim Militär: Der Hightech-Krieger mit GPS-Ortungsgeräten, Echtzeitübertragung von Videolagebildern, nanobeschichteten Titan-Sonnenbrillen, Nachtsichtwärmebildschirmen und lasergesteuerter Munition, wie wir ihn bei den Amerikanern in Afghanistan sehen, droht am Ende doch dem sandalen- und turbantragenden Taliban mit seiner besseren Ortskenntnis, Tarnung und seinem unbedingten Willen zum Sieg zu unterliegen. Dieselbe Lehre zog auch der ehemalige Chief Information Technology Officer der US-Armee, Generalleutnant a. D. Steven Boutelle, der meinte, man solle den Soldaten nicht unnötig vernetzen und mit zu viel Informationen versorgen; alles, was er an Systemen in dieser Beziehung brauche, seien ein Mobiltelefon und flache Hierarchien.[3]

Ähnliche Gefahren des technologischen „Overkill" könnten sich einstellen, wenn man in hochmodernen und hochvernetzten Lagezentren der Zukunft seitens der höheren Führungsebenen der Versuchung nachgeben sollte, von der bewährten Auftragstaktik abzuweichen und von ganz oben nach ganz unten in taktische Belange „an der Front" durchzugreifen. Die Technik kann auch dort das Bild vor lauter scheinbar kompletten Informationen vernebeln und den Einzelnen unflexibel und entscheidungsunfreudig

2 BMBF 2007.
3 BS 2009.





machen. Die unteren Ebenen sind, statt zu handeln, immer mehr damit beschäftigt, Informationen zu sammeln und in das System einzuspeisen. Boutelle stellt fest: „Je mehr Daten und Wissen ein Netzwerk hat, desto träger reagiert es".[4] Was für das Militär gilt, das gilt im übertragenen Sinne auch für zivile Sicherheitskräfte.

Alle genannten Beispiele zeigen, dass Technik dem Menschen dienen muss und nicht umgekehrt. Technik im Einsatz von Sicherheitskräften muss deshalb nicht nur ergonomisch, zuverlässig und angepasst an deren Bedürfnisse sein, sondern diese Einsatzkräfte selbst müssen bestens geschult und an der Technik trainiert sein, um sie „wie im Schlaf" bedienen zu können, besonders in Stresssituationen. Dazu gehört auch ein besseres Zusammenwirken, ein Erzielen von Sprachfähigkeit und echter Interaktion zwischen den vielen Akteuren der zivilen Sicherheit. Praxisnahe Anforderungen an die Technik wie auch leistungsfähige Test- und Simulationszentren bis hin zu einheitlichen Normen und Standards für die Nachfrager, die in zugelassenen Zertifizierungszentren validiert werden, sind deshalb unabdingbar und sollten im Rahmen des nationalen Sicherheitsforschungsprogramms, wenn möglich aber auch gleich auf europäischer Ebene, definiert und initiiert werden. Auf nationaler Ebene in Deutschland wird zu fragen sein, ob sich jede Landespolizei, jeder Wachdienst so etwas leisten kann und ob es nicht für viele Entwicklungen und Produkte der Sicherheitsindustrie zertifizierte und zertifizierungsfähige zentrale Erprobungs-, Zulassungs- und Trainingszentren bundesweit (oder europaweit) geben sollte.



2.3 BESCHAFFUNGSMÄRKTE ORGANISIEREN

Die Forderung nach zentralen, einheitlichen Erprobungs-, Zulassungs- und Trainingszentren für Sicherheitstechnik führt zum Blick auf die Märkte. Der deutsche Markt für Sicherheitstechnologien und seine prognostizierte Entwicklung bis 2015 sowie die deutsche Position und unsere Chancen am Weltmarkt wurden vor Kurzem in einem Gutachten der VDI/VDE Innovation + Technik GmbH im Auftrag des Bundesministeriums für Wirtschaft und Technologie ausführlich dargestellt.[5] Der deutsche Gesamtmarkt wird in dieser Studie auf rund 20 Mrd. Euro im Jahr 2008 geschätzt, wovon deutsche Unternehmen knapp 70 Prozent abdecken. Bis 2015 wird dieser Markt vermutlich auf 31 Mrd. Euro angewachsen sein.[6] Nach einer Studie der Boston Consulting Group aus dem Jahr 2006 wächst der weltweite Markt für Sicherheitstechnik zwischen 2003 und 2014 um 6 Prozent pro Jahr, von 41 Mrd. Dollar auf 86 Mrd. Dollar.[7]

Doch die gegenwärtig laufenden nationalen und europäischen Sicherheitsforschungsprogramme sind von den Märkten noch ein gutes Stück entfernt. Der 2006 durch die Bundesregierung organisierte „Agendaprozess" für eine nationale Sicherheitsforschungsstrategie endete zwar mit einer ausführlichen Beschreibung der Fähigkeiten

4 BS 2009.
5 VDI/VDE 2009.
6 VDI/VDE 2009, S. 180 f.
7 IABG/EMI, S. 34 f.







in Wissenschaft und Industrie auf der einen Seite und der Notwendigkeiten bei den privaten und öffentlichen Nachfragern von Sicherheitstechnik auf der anderen. Anhand von prioritären Bedrohungsszenarien hat man dann die Forschungs- und Entwicklungsbedarfe sortiert und angefangen, die dafür bis 2010 bereitstehenden 123 Mio. Euro im Wettbewerb über Ausschreibungen zu vergeben.[8] Doch wie realistisch die Hoffnung dabei ist, eines Tages zu technischen Lösungen zu kommen, die unsere Gesellschaft sicherer machen und unsere Industrie weltweit im Wettbewerb bestehen lassen, ist weitgehend offen.

Ein vollkommen anderer Ansatz – und ein vielleicht aussichtsreicherer – wäre es gewesen, statt eines ergebnisoffenen Forschungsprogramms ein 120 Mio. Euro-Beschaffungsprogramm für die Behörden und Organisationen mit Sicherheitsaufgaben (BOS) aufzulegen. Die BOS, Betreiber kritischer Infrastrukturen (soweit der Staat noch an ihnen beteiligt ist) und andere wichtige Nachfrager von Sicherheitstechnik hätten definieren können, wie zum Beispiel der Polizist der Zukunft oder der Feuerwehrmann der Zukunft aussehen soll, welche Sicherheitsbedarfe Atomkraftwerke (neben den rein strahlungstechnischen Sicherheitsbedarfen) noch haben oder wie große Rechenzentren vor unerwünschten Zugriffen über das Netz geschützt werden sollen. Es wären umfangreiche Pflichtenhefte entstanden, in denen bestimmte Fähigkeiten (nicht hingegen technische Spezifikationen) definiert werden, die die zukünftigen Systeme erfüllen sollen. Sofern die Industrie in diesen Anforderungen einen interessanten Markt sehen würde, würde sie von alleine investieren, Forschungsaufträge vergeben und Normierungen anstoßen. Am Ende würden Produkte herauskommen, die sich rentieren, und die Endnutzer würden ihre Bedarfe tatsächlich befriedigen können. In groben Zügen wäre dies ein industriepolitischer Ansatz für die Sicherheitswirtschaft, der auch zu verwertbaren Ergebnissen führte.

Die szenarienorientierte Sicherheitsforschung, wie sie derzeit betrieben wird, hat Elemente davon, aber eben auch Elemente einer freien Grundlagenforschung. Der Hauptnachteil an der Sache ist, dass niemand weiß, ob es hinterher einen Markt für die Entwicklungen geben wird. Industriepolitik sieht anders aus. Die öffentliche Hand wird nur in sehr eingeschränktem Maße der Markt sein können. Abgesehen davon, dass es 16 Länderpolizeien und eine Bundespolizei mit jeweils unterschiedlichen Beschaffungsprioritäten und -rhythmen gibt und dadurch kaum nationale Skaleneffekte dafür sorgen, weltmarktfähige Produkte in ausreichend großen Referenzmärkten platzieren zu können, sind die Haushalte der Innenressorts in keiner Weise mit denen des Bundesforschungsministeriums und dessen Programm korreliert. So werden viele der heute arbeitenden Konsortien ihre Entwicklungen entweder anderswo verkaufen müssen, auslizenzieren oder auf bessere Zeiten hoffen. Die Industriepartner haben im besten

[8] BMBF 2007, S. 22-45; siehe auch VDI/VDE 2009, Kapitel 6.







Falle neue Produkte, aber sie haben nicht notwendigerweise neue Kunden. Sicherlich muss man den Gesamtmarkt sehen, und der besteht in Deutschland, aber auch darüber hinaus, zu einem überwiegenden Teil aus privaten Nachfragern. Die BOS machen in Deutschland nur gut ein Viertel der Nachfrage aus.[9] Dennoch kann man eine der Schwächen der gegenwärtigen Forschungspolitik in Deutschland darin sehen, dass sie unter dem Verdikt des Wettbewerbs- und des Vergaberechts nahezu zweckfreie Forschung auf Vorrat anstößt, ohne dass ihr in anderen Ressorts (Inneres, Wirtschaft, vielleicht auch Auswärtiges) auch nur halbwegs angemessene Instrumente entsprechen, um die Forschungsergebnisse auch in wirtschaftlich ertragreiche Betätigungen im Feld der zivilen Sicherheit umzusetzen.

Überspitzt kann man deshalb sagen: Das nationale und auch das europäische Sicherheitsforschungsprogramm werden eine Art Luxusproblem kreieren: Wenn sie tatsächlich grundlagenorientierte Anwendungsforschung sind, also mehr als nur die Wiederauflage und Zusammenschau schon erreichter Ergebnisse der Industrie und der Institute, werden sie Erkenntnisse bereitstellen, die weit über das hinausgehen, was die Nachfrager in der Lage sind, zu beschaffen. Die Fragmentierung des Marktes (bei Nachfragern *und* Anbietern) gebiert fehlende Standardisierung, das Ausbleiben von Größenvorteilen und einen Mangel an Interoperabilität. Der Polizei fehlt das Geld, der Industrie der ausreichend große Markt und den Infrastrukturbetreibern fehlen die einheitlichen Standards. Deutschland braucht deshalb Erkenntnisse, wie Strukturen verbessert, Märkte organisiert, innovative Produkte eingeführt und einheitliche Standards durchgesetzt werden können.

Im ursprünglichen Sinn des Wortes geht es hier also darum, „Technologietransfer“ zu organisieren, denn Innovationen sind Erfindungen plus Markt. In Umsetzung einer EU-Richtlinie ist Anfang dieses Jahres ein neues Vergaberecht in Kraft getreten, das es erlaubt, in Ausschreibungen der öffentlichen Hand auch die Auswahlkategorie „innovativ“ vorzusehen, so dass nicht immer nur der Stand der Technik abgefragt wird, sondern auch ganz Neues, möglicherweise noch nicht ausreichend Validiertes. Auf diese Weise will man dazu beitragen, dass manche der Forschungsergebnisse doch ihre Märkte erhalten, auch wenn es sich nur um erste, noch beschränkte Testmärkte handeln sollte. In dieser Richtung hat auch ein Diskussionspapier argumentiert, das die German European Security Association e.V. (GESA) zu Anlass der Innenministerkonferenz 2008 formuliert hat und das dort informell diskutiert wurde. Ein innovationsfreundliches Vergaberecht zu schaffen ist ein Weg, der weiter ausgebaut werden sollte.

Daneben bedarf es aber auch anderer Elemente einer Industriepolitik für die Sicherheitswirtschaft (das ist auch eine der Schlussfolgerungen der VDI/VDE-Studie 2009, die das BMWi aufgenommen hat und gegenwärtig in Fachkreisen diskutiert)[10]. Als Stichworte seien hier nur aufgezählt: Auflage einer Exportinitiative Sicherheit, Schaffung

9 VDI/VDE 2009, S. 221.
10 Vgl. VDI/VDE 2009, Kapitel 11.







einer Koordinierungsstelle Normierung/Standardisierung bei Sicherheitstechnologien beim DIN und Aufbau eines nationalen Netzwerkes von Kompetenz-Clustern. Hinzufügen könnte man weitere allgemeine wirtschaftsfördernde Maßnahmen wie Existenzgründerförderung (zum Beispiel Ausgründungen aus Hochschulen), Investoren-Akquisition (zum Beispiel aus den USA) und natürlich Technologieförderung (die nicht immer „Forschungs"-Förderung sein muss, sondern marktnahe Entwicklungsförderung).

2.4 DEUTSCHLANDS KRÄFTE BÜNDELN

Was nottut, sind zusammenfassend folgende drei Punkte:

1. ein besseres Verständnis der ganzen Breite und vielfältigen Bezüge der verschiedenen Sphären der zivilen Sicherheit (einschließlich ihrer militärischen Aspekte) und die richtigen Schlussfolgerungen daraus für Technikentwicklung, Kooperation und Organisation;
2. das Bereitstellen interoperabler, standardisierter und validierter Systeme in einem europäischen Markt für zivile Sicherheit, die an die Bedürfnisse der Operateure angepasst sind und für die es ausreichend Erprobung und Training gibt;
3. die Überwindung fragmentierter Märkte zumindest innerhalb Deutschlands, wenn nicht Europas, und die stärkere Verbindung von industriepolitischen Maßnahmen mit den schon in Gang gesetzten Forschungsprogrammen.




Diese drei Herausforderungen müssen an zentraler Stelle organisiert werden, denn interministerielle und Bund-Länder-Arbeitsgruppen stoßen hier an ihre operativen Grenzen. Zu empfehlen ist die Gründung eines Deutsch-Europäischen Sicherheitsinstituts, das sich der Umsetzung der drei genannten Aufgaben (man könnte auch sagen: Behebung der drei genannten Schwachpunkte im System) widmet. Es könnte dies auf drei Ebenen der Arbeit tun:

1. Denkfabrik (wissen, worüber man redet),
2. Transfermanagement (vermitteln, was man weiß und wen man kennt),
3. Prozess- und Projektmanagement (tun, was man sich vorgenommen hat).

Das Institut wäre insofern ein Katalysator, ein Generator und ein Motor der Entwicklung.

Auf Ebene 1 sollte das Institut interdisziplinäre Forschung der Besten auf ihren Gebieten anregen und organisieren (bis hin zum Beibringen von Finanzierungen), die etwas zum Komplex der zivilen Sicherheit zu sagen haben. Das kann in der Form geschehen, dass Marktanalysen, Gutachten und Studien in Auftrag gegeben werden, einschließlich Masterarbeiten, Dissertationen und eigener Forschungsprojekte. Auch kann





dies die Form von kleinen Workshops, größeren Symposien und Tagungen annehmen. Und es kann in Form von Stellungnahmen zu Gesetzesvorhaben, Prognosedaten oder Ereignisanalysen geschehen. Die Verbreitung der Ergebnisse findet einerseits auf dem Wege der Politikberatung statt, andererseits über eine gezielte Presse- und Öffentlichkeitsarbeit.

Auf Ebene 2 sollte der eigentliche Vermittlungsprozess zwischen den Kenntnisträgern aus der technischen und geistes- und sozialwissenschaftlichen Forschung, den Anbietern und den Nachfragern von Sicherheitslösungen stattfinden. Dies ist in beiden Richtungen und möglichst in einer vorausschauenden Form zu initiieren, die technologische und gesellschaftliche Entwicklungen antizipiert und integrierte Strategien und Lösungen von allen Akteuren mit auf den Weg bringt. Ein wesentlicher Aspekt der Arbeit auf dieser Ebene wird es sein, Interessen abzuprüfen, Kooperationspartner zu finden und Projekte zu definieren.

Auf Ebene 3 schließlich sollte das Institut eine Dienstleistung anbieten, die die sonstigen Akteure der zivilen Sicherheit in ihrem Tagesgeschäft bei beschränkten internen Ressourcen nur schwer abdecken könnten. Das ist oftmals das Management von Prozessen und Projekten, gegebenenfalls die Übernahme von Antragsmanagement, im Einzelfall auch die Begleitung und Steuerung von Projekten in der Umsetzungsphase.



Das entscheidende Merkmal des Instituts sollte es sein, dass es keine Eigeninteressen verfolgt und dass es nicht in Konkurrenz zu schon vorhandenen Strukturen, Forschungseinrichtungen und Programmen tritt, sondern sich als „facilitator" versteht, als Anreger, Vermittler und Dienstleister. Nicht eigene Forschung sollte im Vordergrund stehen, sondern die Nutzung und (Be-) Förderung der Kompetenzen in den Wissenschaftseinrichtungen bundesweit.

2.5 FAZIT

Die deutsche Sicherheitsforschung und -industrie ist insgesamt gut aufgestellt. Besonders in der Beherrschung unterschiedlichster Basistechnologien, aber auch in der Systemkompetenz haben deutsche Institute und Unternehmen einiges zu bieten. Das viel zu späte Aufsetzen eines deutschen Sicherheitsforschungsprogramms und das, gemessen an unserem Bruttosozialprodukt und unserem Beitrag zum EU-Budget, schwache bisherige Abschneiden deutscher Projekte im 7. Forschungsrahmenprogramm der EU zeigt jedoch, dass es dringend einer einheitlicheren, zielgerichteteren Politik in diesem Feld bedarf. Innovative Verwaltungsverfahren, eine vorausschauende Organisation und die Überwindung von regionalen und ressortspezifischen Eigenbröteleien sind Voraussetzung dafür, die Kreativität und die Kraft der deutschen Wissenschaft und Wirtschaft zur Geltung bringen zu können.







2.6 LITERATUR

BMBF 2007
Bundesministerium für Bildung und Forschung (Hrsg.): Forschung für die zivile Sicherheit. Programm der Bundesregierung. Bonn, Berlin, 2007.

BS 2009
Behördenspiegel: Die Hightech-Army aus dem Supermarkt. (AFCEA-Sonderausgabe). Bonn, 2009.

IABG/EMI 2008
Ministerium für Wirtschaft des Landes Brandenburg (Hrsg.): Gutachten zu einem Masterplan zur Entwicklung der Region Berlin-Brandenburg zu einem Kompetenzzentrum für Safety and Security. Potsdam: Industrieanlagen-Betriebsgesellschaft mbH und Fraunhofer-Institut für Kurzzeitdynamik Ernst-Mach-Institut (EMI). Potsdam, 2008.

VDI 2009
VDI Technologiezentrum (Hrsg.): Informationsbrief zur Sicherheitsforschung: Hintergründe 1/09: Ergebnisse des 2. Calls im europäischen Sicherheitsforschungsprogramm. Düsseldorf, 2009.



VDI/VDE 2009
VDI/VDE Innovation + Technik GmbH: Marktpotenzial von Sicherheitstechnologien und Sicherheitsdienstleistungen. Thema: Der Markt für Sicherheitstechnologien in Deutschland und Europa – Wachstumsperspektiven und Marktchancen für deutsche Unternehmen. (Studie der VDI/VDE Innovation + Technik GmbH und der Arbeitsgemeinschaft für Sicherheit der Wirtschaft e.V. im Auftrag des Bundesministeriums für Wirtschaft und Technologie). Berlin, 2009.

von Senger und Etterlin 2006
von Senger und Etterlin, Stefan: Security industries: Global context, European efforts and the potential in Berlin-Brandenburg - A short survey, 2. Aufl. Potsdam: Zukunfts-Agentur Brandenburg GmbH, 2006.







> AUTORENVERZEICHNIS

Prof. Dr.-Ing. habil. Dr.-Ing. E.h. Dr. h. c. **Friedrich-Wilhelm Bach** ist seit 2001 Professor für Werkstoffkunde und Direktor des Instituts für Werkstoffkunde und kommissarischer Leiter des Instituts für Kerntechnik und Zerstörungsfreie Prüfverfahren an der Leibniz Universität Hannover. Er studierte an der Technischen Universität Hannover Maschinenbau mit Fachrichtung Werkstofftechnik. 1972 schloss er sein Studium erfolgreich ab. 1978 erfolgte die Promotion zum Dr.-Ing. und 1983 seine Habilitation an der Universität Hannover. Seine berufliche Laufbahn führte ihn über verschiedene Stationen und Einrichtungen. Unter anderem war er Geschäftsführer des Unterwassertechnikums Hannover (UWTH), Leiter der Forschungs- und Ausbildungsstelle Unterwasser- und Umwelttechnik der Hansestadt Greifswald (UTEG), Professor und Inhaber des Lehrstuhls für Werkstofftechnologie an der Universität Dortmund (bis 2001) und ist Mitglied, Gutachter und Vorsitzender in verschiedenen Gremien und Beiräten. Seit 2005 ist Bach Dekan der Fakultät für Maschinenbau an der Leibniz Universität Hannover. 2008 wurde er Mitglied des Vorstandes des Clausthaler Zentrums für Materialtechnik (CZM) und seit 2009 ist Bach Mitglied des Kuratoriums des Niedersächsischen Zentrums für Energietechnik (EFZN).

Prof. Dr. **Gerhard Banse** ist Professor für Philosophie und wissenschaftlicher Mitarbeiter am Forschungszentrum Karlsruhe GmbH Technik und Umwelt, Institut für Technikfolgenabschätzung und Systemanalyse (ITAS). 1965 bis 1969 studierte er Chemie, Biologie und Pädagogik an der Pädagogischen Hochschule Potsdam. Er promovierte 1974 an der Humboldt-Universität zu Berlin im Fach Philosophie und habilitierte 1981 an der Akademie der Wissenschaften der DDR. Bis 1991 war er danach als wissenschaftlicher Mitarbeiter am Institut für Philosophie der Akademie der Wissenschaften der DDR tätig, bis 1999 am Lehrstuhl Technikphilosophie der Brandenburgischen Technischen Universität Cottbus und am Institut für Philosophie der Universität Potsdam. Hinzu kamen in den 1990er Jahren mehrere Gastwissenschaftleraufenthalte an der Heinrich-Heine-Universität Düsseldorf, der Pennsylvania State University, der Europäischen Akademie



zur Erforschung von Folgen wissenschaftlich-technischer Entwicklungen Bad Neuenahr-Ahrweiler und dem damaligen Kernforschungszentrum Karlsruhe. Neben seiner Tätigkeit am ITAS ist Gerhard Banse Honorarprofessor für Allgemeine Technikwissenschaft an der Brandenburgischen Technischen Universität Cottbus und Gastprofessor an der Humanwissenschaftlichen Fakultät der Matej-Bel-Universität Banská Bystrica (Slowakische Republik). Darüber hinaus ist er Mitglied des VDI-Ausschusses „Technikbewertung“ und Vizepräsident der Leibniz-Sozietät der Wissenschaften zu Berlin e. V. Seine Hauptarbeitsgebiete sind Technikphilosophie, Allgemeine Technikwissenschaft und Technikfolgenabschätzung vor allem im Bereich Informations- und Kommunikationstechnologien sowie informationstechnische Sicherheit. Er ist Mitherausgeber diverser Buchreihen und Herausgeber, Mitherausgeber sowie Autor vieler Buch- und Zeitschriftenpublikationen zu den Themen Technik und Risikoforschung.

Prof. Dr.-Ing. **Jürgen Beyerer** ist Leiter des Fraunhofer-Instituts für Informations- und Datenverarbeitung (IITB) in Karlsruhe. Nach seinem Studium der Elektrotechnik an der Universität Karlsruhe (TH) 1989 arbeitete er als wissenschaftlicher Angestellter am Institut für Mess- und Regelungstechnik der Universität Karlsruhe auf dem Gebiet der Bild- und Signalverarbeitung. Für seine 1994 „mit Auszeichnung“ abgeschlossene Promotion zum Thema „Analyse von Riefentexturen“ wurde ihm 1995 der Messtechnikpreis des AHMT verliehen. Ab 1994 arbeitete er als wissenschaftlicher Assistent am Institut für Mess- und Regelungstechnik der Universität Karlsruhe, wo er unter anderem eine Forschungsgruppe auf dem Gebiet der automatischen Sichtprüfung und Bildverarbeitung aufbaute. 1999 habilitierte er im Fach Messtechnik an der Fakultät für Maschinenbau der Universität Karlsruhe und wechselte danach zur mittelständischen Firmengruppe Hottinger in Mannheim. Dort etablierte er die neue Firmentochter Hottinger Systems GmbH mit den Schwerpunkten automatische Sichtprüfung und Robotertechnik, die er auch als Geschäftsführer leitete. Daneben war er bei der Hottinger Maschinenbau GmbH als stellvertretender Geschäftsführer tätig und lehrte an der Universität Karlsruhe als Privatdozent. Neben seiner Ernennung als Leiter des Fraunhofer-IITB wurde Jürgen Beyerer 2004 als ordentlicher Professor an den Lehrstuhl für Interaktive Echtzeitsysteme an der Universität Karlsruhe berufen.





Anna Dahlem studierte nach ihrem Abitur Wirtschaftsingenieurwesen an der Universität Karlsruhe. Seit 2008 ist sie Wissenschaftliche Mitarbeiterin am Fachgebiet für Produktsicherheit und Qualitätswesen von Prof. Dr.-Ing. habil. Petra Winzer an der Bergischen Universität Wuppertal (BUW) Fachbereich D-Abteilung Sicherheitstechnik.



Dr. rer. nat. **Birgit Drees** ist Projektmanagerin für den Fraunhofer Innovationscluster „Future Security BW". Sie promovierte an der Westfälischen Wilhelms-Universität Münster im Fach Biologie. Seit 2008 ist sie am Fraunhofer Ernst-Mach-Institut im Business Development mit dem Schwerpunkt Sicherheitsforschung tätig.

Dr. **Stefan von Senger und Etterlin** leitet seit Juni 2009 die „Brandenburgische Geschäftsstelle zur Umsetzung des Masterplans Sicherheitswirtschaft und -wissenschaft" in der ZukunftsAgentur Brandenburg GmbH (ZAB, www.zab.eu). Er studierte Nordamerikanistik, Politik und Geschichte in Freiburg, Amherst (USA) und Berlin und promovierte an der FU Berlin. Zwischen 1995 und 1998 absolvierte er nebenberuflich im Fernstudium einen MBA am Henley Management College. Wichtige berufliche Stationen waren die EU-Kommission in Brüssel, der US-Kongress in Washington und die Universität Frankfurt/Main. Er war Referent für Presse- und Öffentlichkeitsarbeit im Ministerium für Wirtschaft, bevor er in der Zeit von 1998-2001 als Referatsleiter für Europapolitik und Außenwirtschaft tätig war. Von 2001 bis Mai 2009 war er Leiter des Teams Außenwirtschaft in der ZAB. Seit 2006 befasst er sich mit dem Aufbau des Handlungsfeldes „Sicherheitswirtschaft".




Dr. rer. nat. **Jürgen Geisler** leitet die Abteilung „Interaktive Analyse und Diagnose" am Fraunhofer-Institut für Informations- und Datenverarbeitung (IITB) und ist stellvertretender Leiter des Instituts. Er studierte Luft- und Raumfahrttechnik mit Schwerpunkt Flugzeugbau an der Hochschule (heute Universität) der Bundeswehr in München-Neubiberg. Nach seinem Studienabschluss als Diplom-Ingenieur 1982 leistete er bis 1989 Wehrdienst als Luftfahrzeugtechnischer Offizier und Leiter der technischen Betriebsführung im Jagdbombergeschwader 33 in Büchel/Eifel. Seit 1989 ist er als wissenschaftlicher Angestellter am Fraunhofer-IITB in Karlsruhe tätig, wo er unter anderem an verschiedenen Projekten auf dem Feld der interaktiven Bildauswertung in der luft- und satellitenbildgestützten Aufklärung mitwirkt. 1999 baute er die Forschungsgruppe „Erkennungsunterstützungssysteme" und 2004 die Abteilung „Interaktive Analyse und Diagnose" auf, die er seitdem leitet. Daneben ist er als Koordinator für Verteidigungs- und Sicherheitsforschung für das Fraunhofer-IITB tätig. 2006 promovierte Jürgen Geisler an der Fakultät für Informatik der Universität Karlsruhe (TH). Als Lehrbeauftragter hält er seit 2006 die Vorlesung „Mensch-Maschine-Wechselwirkung in der Anthropomatik" an der Universität Karlsruhe.





Dr. **Andreas Hoffknecht** ist beim VDI-Technologiezentrum in der Abteilung Zukünftige Technologien Consulting tätig. Er studierte Physik an der Justus-Liebig-Universität Gießen und war von 1996 bis 2000 wissenschaftlicher Assistent an der Privatuniversität Witten/Herdecke, bevor er zum VDI-Technologiezentrum wechselte. Als Senior Berater beschäftigt er sich im Rahmen der Technologiefrüherkennung, des Wissensmanagements und der Innovationsbegleitung unter anderem mit den Themen Elektronik, Informationstechnologien, Konvergente Technologien und Sicherheitsforschung. Er hat mehrere Studien für das Bundesministerium für Bildung und Forschung, die EU-Kommission sowie weitere Institutionen und Unternehmen durchgeführt. Andreas Hoffknecht war 2006 maßgeblich an der Vorbereitung des nationalen Sicherheitsforschungsprogramms beteiligt. Seit Start des Programms im Jahr 2007 ist er beim Projektträger Sicherheitsforschung der VDI-Technologiezentrum GmbH für die Innovationsbegleitung verantwortlich.




Prof. Dr. **Gerhard Knorz** ist seit 2002 Vizepräsident der Hochschule Darmstadt für Informations- und Qualitätsmanagement. Er studierte Informatik an der TU Darmstadt (Diplom 1973), wo er 1983 über automatische Inhaltserschließung auf der Grundlage von Text-Mining-Methoden promovierte. Projekte im Bereich Automatische Indexierung, Non-Standard-Datenbanken und Expertensysteme sowie Vertretungsprofessuren Computerlinguistik, Information Retrieval und Datenbanksysteme an den Universitäten Konstanz und Darmstadt gehörten zu seinen folgenden Aufgaben und beruflichen Stationen. 1986 erhielt er eine Professur an der Hochschule Darmstadt für die methodischen Grundlagen professioneller Informationsarbeit. Er ist Gründungsmitglied der GI-Fachgruppe Information Retrieval. Zu seinen weiteren Tätigkeiten gehört die langjährige Arbeit in Vorständen und Beiräten von Fachgesellschaften und Institutionen (GI-FG Information Retrieval, Gesellschaft für Linguistische Datenverarbeitung, Hochschulverband Informationswissenschaft, Information Processing and Management (Pergamon Press), Verband Informations- und Organisationssysteme, Informationszentrum Sozialwissenschaften). Knorz hat zahlreiche Publikationen im Bereich Information Retrieval, Informationswissenschaft, Wissensrepräsentation veröffentlicht. Aktuell arbeitet er im Bereich semantischer Technologien.

Dr. rer. nat. **Tobias Leismann** ist Leiter der Geschäftsstelle des Fraunhofer-Verbunds Verteidigungs- und Sicherheitsforschung (VVS). Er studierte Physik an den Universitäten Heidelberg und Cambridge sowie an der TU München, wo er 2004 promovierte. Nach vier Jahren als Technology Consultant kam er 2008 an das Fraunhofer Ernst-Mach-Institut und übernahm dort die Leitung des Geschäftsfeldes Sicherheitsforschung. Neben seiner Tätigkeit in der Geschäftsstelle des VVS ist Tobias Leismann Geschäftsführer des Fraunhofer Innovationsclusters „Future Security BW".





Dr. **Norbert Pfeil** ist Mitglied des Präsidiums der BAM Bundesanstalt für Materialforschung und -prüfung, Berlin. Er studierte Chemie an der TU Berlin, wo er 1978 promovierte. Bis 2003 war er in der Abteilung Chemische Sicherheitstechnik der BAM in unterschiedlichen fachlichen Bereichen und Positionen tätig, zunächst in der Pyrotechnik, dann als Leiter der Fachgruppe „Reaktionsfähige Stoffe und Stoffsysteme" und zuletzt als Leiter der Abteilung. Auf seinen Arbeitsgebieten Pyrotechnik, Gefahrstoffe/Gefahrgüter, Arbeitsschutz, Anlagensicherheit und Störfallvorsorge war er in nationalen und internationalen Beratungs- und Regelsetzungsgremien aktiv. Nach zwei Berufungsperioden als Vorsitzender des Technischen Ausschusses für Anlagensicherheit (TAA) erhielt er 2006 für die Beratung der Bundesregierung auf dem Gebiet der Anlagensicherheit das Bundesverdienstkreuz. Norbert Pfeil ist derzeit Vorsitzender der ProcessNet-Fachgemeinschaft Sicherheitstechnik und Chairman der „International Group of Experts on the Explosion Risks of Unstable Substances".

Dr. jur. **Thomas Regenfus** ist Habilitand am Institut für Recht und Technik im Fachbereich Rechtswissenschaft der Friedrich-Alexander-Universität Erlangen-Nürnberg. Er war mehrere Jahre wissenschaftlicher Mitarbeiter am Institut für Recht und Technik und ist in dieser Zeit insbesondere durch Publikationen im Bürgerlichen Recht, Zivilprozessrecht und Technikrecht hervorgetreten. 2007 promovierte er mit einer Arbeit über die „Durchsetzung zivilrechtlicher Abwehransprüche bei behördlichen Genehmigungserfordernissen", für die er mit dem Staedtler-Promotionspreis ausgezeichnet wurde. Seit Oktober 2007 ist Thomas Regenfus in der Bayerischen Justiz als Richter bzw. Staatsanwalt tätig.




Prof. Dr. Dr. h. c. **Ortwin Renn** ist Ordinarius für Umwelt- und Techniksoziologie an der Universität Stuttgart und Direktor des zur Universität gehörigen Interdisziplinären Forschungsschwerpunkts Risiko und Nachhaltige Technikentwicklung am Internationalen Zentrum für Kultur- und Technikforschung (ZIRN). Seit 2006 bekleidet er das Amt des Prodekans der Wirtschafts- und Sozialwissenschaftlichen Fakultät und ist Geschäftsführender Direktor des Instituts für Sozialwissenschaften. Neben seinem Engagement an der Universität Stuttgart gründete Renn das Forschungsinstitut DIALOGIK, eine gemeinnützige GmbH, deren Hauptanliegen in der Erforschung und Erprobung innovativer Kommunikations- und Partizipationsstrategien in Planungs- und Konfliktlösungsfragen liegt. Nach seiner Ausbildung in Volkswirtschaftslehre, Soziologie und Sozialpsychologie und anschließender Promotion in Köln arbeitete Renn als Wissenschaftler und Hochschullehrer in Deutschland, den USA und der Schweiz. Seine berufliche Laufbahn führte ihn über das Forschungszentrum Jülich, eine Professur an der Clark University in Worchester/Massachusetts (USA) und eine Gastprofessur an der ETH Zürich nach Stuttgart. Von 1998 bis 2003 leitete er die Akademie für Technikfolgenabschätzung in Baden-Württemberg. Ortwin Renn verfügt über eine mehr als dreißigjährige Erfahrung





auf dem Feld der Risikoforschung, der Technikfolgenabschätzung sowie der Einbindung von Interessengruppen und der allgemeinen Öffentlichkeit bei der Lösung konfliktgeladener Themen. Ortwin Renn hat zahlreiche Preise und Auszeichnungen erhalten. Unter anderem erhielt er die Ehrendoktorwürde der ETH Zürich (Dr. sc h.c.) und den „Distinguished Achievement Award" der Internationalen Gesellschaft für Risikoanalyse (SRA). Er ist Mitglied nationaler und internationaler Akademien der Wissenschaft (z. B. der Berlin-Brandenburgischen Akademie der Wissenschaften, des Panels on Public Participation der US Academy of Science und der Nationalen Academy of Disaster Reduction and Emergency Management of the People's Republic of China). Renn ist ebenfalls Mitglied des Präsidiums von acatech – Deutsche Akademie der Technikwissenschaften. Seit 2005 leitet er den Nachhaltigkeitsbeirat des Landes Baden-Württemberg.





Privatdozent Dr.-Ing. habil. **Wolfram Risch** ist Geschäftsführer der ATB GmbH Chemnitz. Von 1967 bis 1974 absolvierte er ein Studium und Forschungsstudium an der damaligen Technischen Hochschule Karl-Marx-Stadt in der Fachrichtung Ergonomie und Arbeitsgestaltung. In den darauffolgenden Jahren bis 1983 war er in der industriepraktischen Arbeit im Fahrzeug- und Maschinenbau mit Schwerpunkt Personalentwicklung und Organisationsgestaltung tätig. 1983 bis 1992 war er wissenschaftlicher Oberassistent und Dozent an der Technischen Universität Chemnitz, wo er 1988 zum Dr. sc. techn. promovierte und drei Jahre später zum Dr.-Ing. habilitierte. 1992 übernahm er die Geschäftsführung der ATB GmbH Chemnitz sowie die wissenschaftliche Leitung für die Bearbeitung von Forschungsprojekten. Wolfram Risch ist Mitglied diverser wissenschaftlicher Beiräte und Kuratorien. Zudem ist er als Gutachter des Bundesministeriums für Bildung und Forschung (BMBF) und des Ministeriums für Wirtschaft, Mittelstand und Energie (MWME) des Landes Nordrhein-Westfalen tätig.

Prof. em. Dr. **Annely Rothkegel** war bis 2009 Professorin für Angewandte Sprachwissenschaft/Technikkommunikation an der TU Chemnitz und ist seit Kurzem Angehörige der TU Chemnitz im Ruhestand. An der Universität des Saarlandes studierte sie Germanistik, Geographie, Philosophie und Kunst und promovierte 1973 im Fach Linguistik. Bis 1986 war sie daraufhin an der Universität Saarbrücken im Sonderforschungsbereich 100, Elektronische Sprachforschung tätig. 1992 habilitierte sie im Fach Allgemeine Sprachwissenschaft/Computerlinguistik und folgte 1994 dem Ruf auf eine Professur für Textproduktion an der FH Hannover, Studiengang Technische Redaktion, die sie bis 2003 ausübte. 2003 bis 2009 hatte sie den Lehrstuhl für Angewandte Sprachwissenschaft/Technikkommunikation an der TU Chemnitz inne. Ihre Forschungsthemen umfassen die Bereiche Textanalyse, Textproduktion, Hypertext, Fach- und Technikkommu-





nikation, Wissen und Terminologie, Risikokommunikation und Sicherheitskultur. Sie hat an verschiedenen Forschungsprojekten zu diesen Themen mitgewirkt, unter anderem an dem BMBF-Projekt HTP (Hypertextproduktion, abgeschlossen 1997), NORMA (Nutzerorientiertes Risikomanagement, abgeschlossen 2003) und dem EU-Projekt MULTH (Multilingualer Thesaurus, abgeschlossen 2008). Darüber hinaus ist Annely Rothkegel Mitherausgeberin der Serie „Text, Translation, Computational Processing" (TTCP) bei Mouton de Gruyter, Berlin.

Prof. Dr.-Ing. Dr. h.c. **Eckehard Schnieder** ist Professor an der Technischen Universität Braunschweig, Institut für Verkehrssicherheit und Automatisierungstechnik. Er studierte Elektrotechnik an der Technischen Universität Braunschweig und promovierte dort im Bereich Antriebstechnik. Von 1979 bis 1989 war er bei Siemens für automatische Bahnsysteme verantwortlich. Seit 1989 lehrt und forscht er an der Technischen Universität Braunschweig in den Bereichen Reglungs- und Automatisierungstechnik sowie Verkehrssicherheit und leitet das zugehörige Institut. Eckehard Schnieder hat zahlreiche nationale und internationale Forschungs- und Entwicklungsprojekte der Verkehrsautomatisierung und -sicherheit initiiert oder an ihnen mitgewirkt.





Dipl. Wirtsch.-Ing. **Lars Schnieder** ist seit 2008 bei Siemens Industry Mobility Rail Automation im Bereich Safety Management für Systeme der Eisenbahnsicherungstechnik tätig. Er absolvierte ein Studium zum Diplom-Wirtschaftsingenieur in der Fachrichtung Bauingenieurwesen an der Technischen Universität Braunschweig und der University of Nebraska in Omaha, USA. Von 2005 bis 2008 war er als Produktmanager für Kunden- und Mitarbeiterschulungen bei der Siemens Rail Automation Academy tätig. Schwerpunkt seiner Arbeit bildete neben der inhaltlichen und didaktischen Konzeption technischer Seminare ihre organisatorische Koordination im Rahmen internationaler Kundenprojekte. Berufsbegleitend zu seiner Beschäftigung bei Siemens Industry Mobility Rail Automation, die er 2008 antrat, promoviert er zurzeit an der Technischen Universität Braunschweig. Sein Forschungsthema ist eine methodische Vorgehensweise zur Erstellung einer konsistenten, widerspruchsfreien und verständlichen Spezifikation automatisierungstechnischer Systeme.

Steffen Tanneberger ist Wissenschaftlicher Assistent am Lehrstuhl von Prof. Dr. Würtenberger sowie von Prof. Eser am Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg. Nach seinem Abitur und Zivildienst studierte er Rechtswissenschaft in Freiburg. Seit 2009 ist er Wissenschaftlicher Assistent und geht einem Promotionsvorhaben bei Prof. Dr. Würtenberger auf dem Gebiet des Sicherheitsrechts nach.



Dr. **Olav Teichert** ist seit 2004 Technologieberater bei der VDI Technologiezentrum GmbH. Er studierte Chemie an der Ruhr-Universität Bochum, promovierte dort im Jahr 2000 und sammelte anschließend berufliche Erfahrungen unter anderem im Bereich der Technologie- und Patentberatung. Schwerpunkte seiner Arbeit beim VDI Technologiezentrum sind Technologiemonitoring und -früherkennung, Roadmapping und Innovationsbegleitung. Seine Forschungsschwerpunkte liegen in den Bereichen Sicherheitsforschung, Energietechnologien, Materialwissenschaften, Weiße Biotechnologie sowie Konvergente Technologien. Olav Teichert hat Studien für das Bundesministerium für Bildung und Forschung (BMBF), die EU sowie weitere Institutionen und Unternehmen durchgeführt. Dazu zählt unter anderem die Studie „Nutzung der Nanotechnologie für sicherheitstechnische Anwendungen" im Auftrag des BMBF. Seit Anfang 2007 betreut er zudem im Auftrag des BMBF die Innovationsbegleitenden Maßnahmen im Rahmen des Sicherheitsforschungsprogramms.




Prof. Dr. rer. nat. **Klaus Thoma** leitet seit 1996 das Fraunhofer Institut für Kurzzeitdynamik, Ernst-Mach-Institut (EMI), das sich speziell mit Stoßwellenphänomenen, Impakt- und Penetrationsvorgängen und der zugehörigen Simulation und Messtechnik befasst. Nach dem Physikstudium und der Promotion an der TU München wechselte er in die Industrie. Nach achtjähriger Industrietätigkeit bei MBB (heute EADS), zuletzt als Abteilungsleiter, war er Mitgründer und Geschäftsführer einer Firma, die sich mit der Entwicklung und Anwendung von Software für den Bereich der nichtlinearen Strukturdynamik befasste. 1994 erhielt er einen Ruf an die Universität der Bundeswehr in München. 1996 wurde Klaus Thoma Direktor des Ernst-Mach-Instituts der Fraunhofer Gesellschaft. 1999 folgte seine Ernennung zum Honorarprofessor für Kurzzeitdynamik an der Fakultät für Bau- und Vermessungswesen der Universität der Bundeswehr in München. 2003 wurde er Honorarprofessor an der „Nanjing University of Science and Technology" in China. Seit 2002 leitet der den Fraunhofer Verbund für Verteidigungs- und Sicherheitsforschung. Als Mitglied des Vorstands der „Carl-Cranz-Gesellschaft für technisch-wissenschaftliche Weiterbildung" engagiert er sich zudem im Bereich der Wissenspflege und der Weiterbildung im Ingenieurbereich. Seit 2007 ist Klaus Thoma Mitglied des „Editorial Advisory Board" des „International Journal of Impact Engineering". Als Vorsitzender des wissenschaftlichen Programmausschusses berät er das BMBF im Bereich er Sicherheitsforschung. Seine Forschungsschwerpunkte liegen in den Bereichen Sicherheitsforschung (Security), Werkstoffmodellierung (Festigkeit, Versagen) bei schnellen Belastungen, Stoßwellenphänomene, Impakt- und Strömungsvorgänge, Numerische Simulation und nichtlineare Finite Methoden, Crash-Analysen in Experiment und Simulation und schließlich Ballistik.





Prof. Dr. jur. **Klaus Vieweg** ist Inhaber des Lehrstuhls für Bürgerliches Recht, Rechtsinformatik, Technik- und Wirtschaftsrecht sowie Direktor des Instituts für Recht und Technik des Fachbereichs Rechtswissenschaft der Friedrich-Alexander-Universität Erlangen-Nürnberg. Nach seinem Jura- und Sportstudium in Bielefeld und Münster promovierte und habilitierte er in Münster. Seine Lehrbefugnis umfasst das Bürgerliche Recht, das Handels- und Gesellschaftsrecht, das deutsche und internationale Wirtschaftsrecht sowie das Zivilprozessrecht. Forschungsaufenthalte in London, Dublin, Utrecht und Kopenhagen sowie die Referendarwahlstation an der Deutsch-Mexikanischen Industrie- und Handelskammer in Mexiko City kamen ergänzend zu seiner akademischen Ausbildung hinzu. Vor dem Antritt seiner Professur in Erlangen war er Professor an der Wirtschaftswissenschaftlichen Fakultät der KU Eichstätt in Ingolstadt. Zu seinen Forschungsschwerpunkten zählen unter anderem das Technik- und Wirtschaftsrecht, mit europäischem und internationalem Bezug. Seit 2005 ist Klaus Vieweg Mitglied von acatech – Deutsche Akademie der Technikwissenschaften.



Prof. Dr.-Ing. habil. **Petra Winzer**, geb. 1955, studierte Elektrotechnik und Arbeitsingenieurwesen und promovierte 1985 in der Sektion Arbeitswissenschaften an der TU Dresden. Nach langjähriger Dozenten-, Forschungs- und Beratungstätigkeit zum Aufbau und zur Umsetzung von integrierten Managementsystemen sowie externer Habilitation an der TU Berlin auf dem Gebiet der Qualitätswissenschaft, leitet sie seit Februar 1999 das Fachgebiet Produktsicherheit und Qualitätswesen an der Bergischen Universität Wuppertal (BUW) Fachbereich D-Abteilung Sicherheitstechnik und ist seit September 2008 Prorektorin für Transfer und Internationales der BUW.



Prof. Dr. **Thomas Würtenberger** ist Inhaber des Lehrstuhls für Staats- und Verwaltungsrecht an der Albert-Ludwigs-Universität Freiburg. Er studierte Rechtswissenschaft in Genf, Berlin und Freiburg sowie an der Ecole Nationale d’Administration in Paris. 1971 promovierte er in Freiburg mit einer Arbeit über „Die Legitimität staatlicher Herrschaft“ und habilitierte 1977 in Erlangen. 1979/80 war er Professor für Öffentliches Recht an der Juristischen Fakultät der Universität Augsburg, worauf 1981 bis 1988 eine Professur an der Universität Trier folgte, bis er 1988 Professor an der Universität Freiburg wurde. Zudem nahm er Gastprofessuren wahr unter anderem an der Faculté de Droit, Paris I (Sorbonne), an der Faculté de Droit in Straßburg sowie als Professeur invité an der Faculté de Droit in Lausanne. 1994 bis 1997 war er im Vorstand des Frankreich-Zentrums der Universität Freiburg tätig. Seit 1997 ist er Rechtsberater des Rektors der Universität Freiburg sowie seit 2002 korrespondierendes Mitglied der Mainzer Akademie der Wissenschaften und der Literatur. Darüber hinaus ist er Mitglied verschiedener Arbeitskrei-



se zur Sicherheitsforschung, unter anderem seit 2007 im Freiburger Kompetenzverbund „Sicherheit und Gesellschaft“. Seine Forschungsschwerpunkte sind neben Staats- und Verwaltungsrecht, vergleichendem Verfassungsrecht und neuerer Verfassungsgeschichte auch die Staatsphilosophie, vor allem Legitimationslehren und die sozialpsychologischen Grundlagen von Staat und Recht. Thomas Würtenberger hat zahlreiche Publikationen zum Polizeirecht und Recht der inneren Sicherheit verfasst.

Dr. Dr. **Axel Zweck** ist Abteilungsleiter der Zukünftige Technologien Consulting der VDI Technologiezentrum GmbH. Er studierte 1979 bis 1987 Chemie sowie 1981 bis 1988 Sozialwissenschaften und Philosophie an der Universität Düsseldorf, wo er 1989 er im Fachbereich Biochemie zum Dr. rer. nat. promovierte. 1992 erfolgte die Promotion zum Dr. rer. phil. im Fachbereich Sozialwissenschaften. Seit 1989 ist er beim VDI Technologiezentrum tätig, wo er 1992 die Leitung der Zukünftige Technologien Consulting übernahm. Schwerpunkt seiner gegenwärtigen Tätigkeit ist die Koordination von Forschungsprojekten und innovationsbegleitenden Maßnahmen, wozu die Beratung des Bundesministeriums für Bildung und Forschung und das Implementieren innovations-, technologie- sowie forschungspolitischer Strategien gehört. Seine Hauptarbeitsgebiete sind Technologiemanagement, Technikbewertung, Technologiefrüherkennung und -monitoring, Zukunftsforschung, Innovationsforschung sowie Forschungs- und Technologiepolitik. Seit 2002 ist er Mitglied des Kuratoriums des Fraunhofer-Instituts für naturwissenschaftliche Trendanalysen in Euskirchen und seit 2004 auch des Fraunhofer-Instituts für physikalische Messtechnik in Freiburg. Seit 2002 nimmt er regelmäßig Lehraufträge am Sozialwissenschaftlichen Institut der Universität Düsseldorf wahr.










> acatech – DEUTSCHE AKADEMIE DER TECHNIKWISSENSCHAFTEN

acatech vertritt die Interessen der deutschen Technikwissenschaften im In- und Ausland in selbstbestimmter, unabhängiger und gemeinwohlorientierter Weise. Als Arbeitsakademie berät acatech Politik und Gesellschaft in technikwissenschaftlichen und technologiepolitischen Zukunftsfragen. Darüber hinaus hat es sich acatech zum Ziel gesetzt, den Wissenstransfer zwischen Wissenschaft und Wirtschaft zu erleichtern und den technikwissenschaftlichen Nachwuchs zu fördern. Zu den Mitgliedern der Akademie zählen herausragende Wissenschaftler aus Hochschulen, Forschungseinrichtungen und Unternehmen. acatech finanziert sich durch eine institutionelle Förderung von Bund und Ländern sowie durch Spenden und projektbezogene Drittmittel. Um die Akzeptanz des technischen Fortschritts in Deutschland zu fördern und das Potenzial zukunftsweisender Technologien für Wirtschaft und Gesellschaft deutlich zu machen, veranstaltet acatech Symposien, Foren, Podiumsdiskussionen und Workshops. Mit Studien, Empfehlungen und Stellungnahmen wendet sich acatech an die Öffentlichkeit. acatech besteht aus drei Organen: Die Mitglieder der Akademie sind in der Mitgliederversammlung organisiert; ein Senat mit namhaften Persönlichkeiten aus Industrie, Wissenschaft und Politik berät acatech in Fragen der strategischen Ausrichtung und sorgt für den Austausch mit der Wirtschaft und anderen Wissenschaftsorganisationen in Deutschland; das Präsidium, das von den Akademiemitgliedern und vom Senat bestimmt wird, lenkt die Arbeit. Die Geschäftsstelle von acatech befindet sich in München; zudem ist acatech mit einem Hauptstadtbüro in Berlin vertreten.



Weitere Informationen unter www.acatech.de

> acatech DISKUTIERT

Die Reihe „acatech diskutiert" dient der Dokumentation von Symposien, Workshops und weiteren Veranstaltungen der Deutschen Akademie der Technikwissenschaften. Darüber hinaus werden in der Reihe auch Ergebnisse aus Projektarbeiten bei acatech veröffentlicht. Die Bände dieser Reihe liegen generell in der inhaltlichen Verantwortung der jeweiligen Herausgeber und Autoren.



BISHER SIND IN DER REIHE „acatech DISKUTIERT" FOLGENDE BÄNDE ERSCHIENEN:

Martina Ziefle, Eva-Maria Jakobs: *Wege zur Techniksozialisation. Sozialisationsverläufe und Interventionszeitpunkte* (acatech diskutiert), Heidelberg u. a.: Springer Verlag 2009.

Thomas Schmitz-Rode (Hrsg.): *Runder Tisch Medizintechnik. Wege zur beschleunigten Zulassung und Erstattung innovativer Medizinprodukte* (acatech diskutiert), Heidelberg u. a.: Springer Verlag 2009.

Otthein Herzog/Thomas Schildhauer (Hrsg.): *Intelligente Objekte. Technische Gestaltung – Wirtschaftliche Verwertung – Gesellschaftliche Wirkung* (acatech diskutiert), Heidelberg u. a.: Springer Verlag 2009.

Thomas Bley (Hrsg.): *Biotechnologische Energieumwandlung. Gegenwärtige Situation, Chancen und Künftiger Forschungsbedarf* (acatech diskutiert), Heidelberg u. a.: Springer Verlag 2009.

Joachim Milberg (Hrsg.): *Förderung des Nachwuchses in Technik und Naturwissenschaft. Beiträge zu den zentralen Handlungsfeldern* (acatech diskutiert), Heidelberg u. a.: Springer Verlag 2009.

Norbert Gronau/Walter Eversheim (Hrsg.): *Umgang mit Wissen im interkulturellen Vergleich. Beiträge aus Forschung und Unternehmenspraxis* (acatech diskutiert), Stuttgart: Fraunhofer IRB Verlag 2008.

Martin Grötschel/Klaus Lucas/Volker Mehrmann (Hrsg.): *Produktionsfaktor Mathematik. Wie Mathematik Technik und Wirtschaft bewegt* (acatech diskutiert), Heidelberg u. a.: Springer Verlag 2008.

Thomas Schmitz-Rode (Hrsg.): *Hot Topics der Medizintechnik. acatech Empfehlungen in der Diskussion* (acatech diskutiert), Stuttgart: Fraunhofer IRB Verlag 2008.

Hartwig Höcker (Hrsg.): *Werkstoffe als Motor für Innovationen* (acatech diskutiert), Stuttgart: Fraunhofer IRB Verlag 2008.

Friedemann Mattern (Hrsg.): *Wie arbeiten die Suchmaschinen von morgen? Informationstechnische, politische und ökonomische Perspektiven* (acatech diskutiert), Stuttgart: Fraunhofer IRB Verlag 2008.



Klaus Kornwachs (Hrsg.): *Bedingungen und Triebkräfte technologischer Innovationen* (acatech diskutiert), Stuttgart: Fraunhofer IRB Verlag 2007.

Hans Kurt Tönshoff/Jürgen Gausemeier (Hrsg.): *Migration von Wertschöpfung. Zur Zukunft von Produktion und Entwicklung in Deutschland* (acatech diskutiert), Stuttgart: Fraunhofer IRB Verlag 2007.

Andreas Pfingsten/Franz Rammig (Hrsg.): *Informatik bewegt! Informationstechnik in Verkehr und Logistik* (acatech diskutiert), Stuttgart: Fraunhofer IRB Verlag 2007.

Bernd Hillemeier (Hrsg.): *Die Zukunft der Energieversorgung in Deutschland. Herausforderungen und Perspektiven für eine neue deutsche Energiepolitik* (acatech diskutiert), Stuttgart: Fraunhofer IRB Verlag 2006.

Günter Spur (Hrsg.): *Wachstum durch technologische Innovationen. Beiträge aus Wissenschaft und Wirtschaft* (acatech diskutiert), Stuttgart: Fraunhofer IRB Verlag 2006.

Günter Spur (Hrsg.): *Auf dem Weg in die Gesundheitsgesellschaft. Ansätze für innovative Gesundheitstechnologien* (acatech diskutiert), Stuttgart: Fraunhofer IRB Verlag 2005.

Günter Pritschow (Hrsg.): *Projektarbeiten in der Ingenieurausbildung. Sammlung beispielgebender Projektarbeiten an Technischen Universitäten in Deutschland* (acatech diskutiert), Stuttgart: Fraunhofer IRB Verlag 2005.



